

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Atsuji SEKIGUCHI

Application No.: Unassigned

Group Art Unit: Unassigned

Filed: February 25, 2004

Examiner: Unassigned

For: ROUTING LOOP DETECTION PROGRAM AND ROUTING LOOP DETECTION
METHOD

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-326173

Filed: September 18, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date(s) as evidenced by the certified papers attached hereto, in accordance with the
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 25, 2004

By: 

David M. Pitcher

Registration No. 25,908

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 9月18日
Date of Application:

出願番号 特願2003-326173
Application Number:

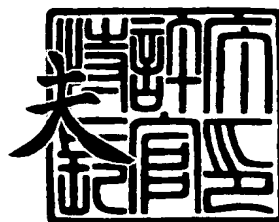
[ST. 10/C]: [JP 2003-326173]

出願人 富士通株式会社
Applicant(s):

2003年12月18日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



出証番号 出証特2003-3105347



【書類名】 特許願
【整理番号】 0351732
【提出日】 平成15年 9月18日
【あて先】 特許庁長官 殿
【国際特許分類】 G06F 13/00
H04L 12/28
H04L 12/56
H04L 29/14

【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社
内
【氏名】 関口 敦二

【特許出願人】
【識別番号】 000005223
【氏名又は名称】 富士通株式会社

【代理人】
【識別番号】 100098235
【弁理士】
【氏名又は名称】 金井 英幸
【電話番号】 03-5283-3188

【手数料の表示】
【予納台帳番号】 062606
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9908696

【書類名】 特許請求の範囲**【請求項 1】**

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出手段、

前記パケット抽出手段が抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先 IP アドレスを読み取る読取手段、

前記読取手段が読み取った送信先 IP アドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信手段、

前記パケット送信手段が送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信手段、及び、

前記パケット受信手段が受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティンググループが発生している旨を出力する出力手段

として機能させる

ことを特徴とするルーティンググループ検出プログラム。

【請求項 2】

前記調査用パケットは、アプリケーション層上に存在するネットワークアプリケーションサービスについてのサービス要求パケットである

ことを特徴とする請求項 1 記載のルーティンググループ検出プログラム。

【請求項 3】

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数を IP ヘッダ中に有するパケットの個数を、計数する計数手段、

前記計数手段が計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別手段、及び、

前記判別手段が前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティンググループの発生の兆候がある旨を出力する出力手段

として機能させる

ことを特徴とするルーティンググループ検出プログラム。

【請求項 4】

コンピュータが、

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出ステップと、

前記パケット抽出ステップにおいて抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先 IP アドレスを読み取る読取ステップと、

前記読取ステップにおいて読み取った送信先 IP アドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信ステップと、

前記パケット送信ステップにおいて送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信ステップと、

前記パケット受信ステップにおいて受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティンググループが発生している旨を出力する出力ステップと

を実行する

ことを特徴とするルーティンググループ検出方法。

【請求項 5】

コンピュータが、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数を IP ヘッダ中に有するパケットの個数を、計数する計数ステップと、

前記計数ステップにおいて計数したホップ数毎のパケットの個数に基づくヒストグラム

において、平坦部又は鋸歯状部の有無を判別する判別ステップと、

前記判別ステップにおいて前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティンググループの発生の兆候がある旨を出力する出力ステップと
を実行する
ことを特徴とするルーティンググループ検出方法。

【書類名】明細書

【発明の名称】ルーティンググループ検出プログラム及びルーティンググループ検出方法

【技術分野】

【0001】

本発明は、ルーティンググループを検出するための装置としてコンピュータを機能させるルーティンググループ検出プログラムと、このようなルーティンググループ検出プログラムが実行されたコンピュータにより実現されるルーティンググループ検出方法とに、関する。

【背景技術】

【0002】

周知のように、インターネットやイントラネット等におけるネットワーク層プロトコルとして、TCP/IP[Transmission Control Protocol/Internet Protocol]スイートに含まれるIPが、広く利用されている。

【0003】

このIPに従った通信機能を有するコンピュータには、他のコンピュータの中から個別に識別するためのIPアドレスが、少なくとも1つ与えられている。この種のコンピュータは、OSI[Open System Interconnection]参照モデルにおけるネットワーク層においてデータを送信する際、その送信データを、パケットと呼ばれる（データグラムとも言う）小さなデータの塊に分割し、送信元及び送信先のIPアドレスやその他の情報をヘッダ情報として各パケットに組み込んで、送信先のコンピュータへ向けて送信する。

【0004】

また、この種のコンピュータは、同種の他のコンピュータと直接接続されていることは少なく、通常、パケットの中継を専門に行う複数のコンピュータを介して接続されている。この中継専門のコンピュータは、一般に、ルータと称されており、これらルータにも、IPアドレスが与えられている。

【0005】

各ルータは、パケットの送信先IPアドレスとそのパケットの送信を担当する他のルータやコンピュータのIPアドレスとを対応付けたルーティングテーブルを、有しており、他のルータやコンピュータからパケットを受信すると、そのルーティングテーブルを参照して、次にパケットを送り渡すルータやコンピュータを選定して送信する。この結果、パケットは、幾つかのルータを経由して送信元のコンピュータから送信先のコンピュータへと順次送られる。

【0006】

また、各ルータは、他のルータやコンピュータからパケットを受信すると、そのパケットのIPヘッダ中の所定フィールド（IPバージョン4では生存時間、IPバージョン6ではホップリミット）に記録される残存ホップ数から1を減じるとともに、IPバージョン4に限りチェックサムフィールドの値を1増加させて、そのパケットを次のルータやコンピュータへ送信する。さらに、各ルータは、残存ホップ数が0になったパケットを破棄してパケット破棄の旨をICMP[Internet Control Message Protocol]に従って送信元IPアドレスのコンピュータへ通知する処理も行う。

【0007】

このようなルータやコンピュータによってIPに従ったパケット通信をネットワーク層において行うことができるネットワークは、一般に、IPネットワークと称されている。

【0008】

ところで、このIPネットワークにおいて生じる通信障害の一つに、ルーティンググループがある。このルーティンググループは、パケットが複数のルータ間を繰り返し巡回することによって送信先に届かなくなるという現象である。

【0009】

このルーティンググループは、手作業により行われる各種設定の間違いやルータ等のハードウェアの故障やその他の障害に因り生じてしまうことが多いが、そのルーティンググループを引き起こしているルータ群を管理する管理者の管理区域外のルータの設定に因って引

き起こされることもある。通常、管理区域外のルータの設定を確認又は変更することはできないので、結局のところ、ルーティンググループは防ぎようのない現象となっている。

【0010】

そこで、このようなルーティンググループの発生に因って管理者に及ぼされる損害を低く抑えるためには、ルーティンググループを発生させているルータ群を如何に素早く発見するかが、重要となってくる。

【0011】

従来、このようなルーティンググループを発見するため、以下に説明する3つの方法が知られていた。

【0012】

第1の方法は、ルーティングテーブルを用いる方法である。すなわち、この第1の方法は、管理区域内の全ルータの有するルーティングテーブルを付き合わせてループを形成しているエントリーレコードの組み合わせを1つずつ探し出すという方法である。この第1の方法には、ループを形成している組み合わせを確実に検出できるという利点がある。

【0013】

第2の方法は、トレースルートを用いる方法である。すなわち、この第2の方法は、トレースルート機能を有するコンピュータを管理区域内のルータに接続してそのコンピュータから管理区域内の別のコンピュータへ残存ホップ数が1ずつ異なる調査用のパケットを順次送信するという方法である。この第2の方法では、当該コンピュータは、送信先のコンピュータまでの経路に存在する各ルータから送られてくる時間超過メッセージ付きパケット（タイプフィールドに11を持つICMPヘッダがIPヘッダに付加されたパケット）のうち、同じルータ群から繰り返し送られてきたものがある場合、そのルータ群においてルーティンググループが発生していると検出する。この第2の方法には、管理区域内の全ての経路においてルーティンググループを検出できるという利点がある。

【0014】

第3の方法は、パケットキャプチャを用いる方法である。すなわち、この第3の方法は、パケットキャプチャ機能を有するコンピュータを管理区域内のルータ間に設置してそのルータ間を通過する全てのパケットを監視するという方法である（例えば非特許文献1参照）。この第3の方法では、当該コンピュータは、IPヘッダ中の残存ホップ数（IPバージョン4の場合にはチェックサム値も）以外の内容が同一であるパケットをそれぞれ抽出し、抽出した各パケットの残存ホップ数（及びチェックサム値）が等差数列的に変化している場合に、ルーティンググループが発生していると検出する。この第3の方法には、即時にルーティンググループを検出できるという利点がある。

【非特許文献1】ウルス＝ヘンガルトナー（Urs Hengartner），スー＝ムーン（Sue Moon），リチャード＝モルティエ（Richard Mortier），クリストフ＝ダイオット（Christophe Diot），“パケット経路中のルーティンググループの検出と解析（Detection and Analysis of Routing Loops in Packet Traces）”，第3頁第4章ルーティンググループの検出（IV Routing Loop Detection），[online]，平成15年6月9日，インターネット<URL：<http://www-2.cs.cmu.edu/People/uhengart/imw02.pdf>>

【発明の開示】

【発明が解決しようとする課題】

【0015】

しかしながら、上述した第1の方法によると、エントリーレコードの組み合わせを1つずつ手作業にて確認せねばならないため、ルーティンググループが発見されるまでに非常に時間がかかる。また、通常のルーティングテーブルのエントリー数が例えば100個のように非常に多いため、管理区域内のルータの数が増えれば増えるほど、ルーティンググループを探し出す作業には、時間と手間が掛かることとなる。従って、この第1の方法は、即時性及び規模拡張性に優れないという問題があった。

【0016】

また、上述した第2の方法によると、或る送信元IPアドレスからのパケットだけがルーティンググループを引き起こしてその他のパケットは引き起こさないという現象が、ルーティングテーブルの一部の間違いによって引き起こされ得るが、この場合、いくら調査用のパケットを経路に流してもルーティンググループを検出することができないことがある。また、調査用のパケットは極めて大量に必要であるため、調査間隔を短くすればするほど、ネットワークトラフィックに多大な負荷を与えることとなり、新たな通信障害を引き起こす虞がある。従って、この第2の方法は、確実性及び即時性に優れないという問題があった。

【0017】

さらに、上述した第3の方法によると、パケットキャプチャを跨いでいるルータ間で発生するルーティンググループについては確実に検出できるものの、パケットキャプチャを跨いでいないルータ間で発生するルーティンググループについては、検出することができない。そのうえ、ルータ間の通信速度が向上すればするほど、パケットキャプチャが取得するパケット数が増加してコンピュータの処理が追いつかなくなるため、iDC [internet Data Center] やISP [Internet Service Provider] などのように通信速度が早い大規模な管理区域に対して、当該コンピュータを適用することができない。従って、この第3の方法は、確実性及び規模拡張性に優れないという問題があった。

【0018】

本発明は、上述したような従来の事情に鑑みてなされたものであり、その課題は、ネットワークの規模の大小に拘わらずルーティンググループを確実に即時に検出するための装置としてコンピュータを機能させるルーティンググループ検出プログラムと、このようなルーティンググループ検出プログラムが実行されたコンピュータにより実現されるルーティンググループ検出方法とを、提供することにある。

【課題を解決するための手段】

【0019】

上記の課題を解決するために、本発明の第1の態様によるルーティンググループ検出プログラムは、以下のような構成を採用した。

【0020】

すなわち、本発明の第1の態様によるルーティンググループ検出プログラムは、コンピュータを、ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をIPヘッダ中に有するパケットの個数を、計数する計数手段、前記計数手段が計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別手段、及び、前記判別手段が前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティンググループの発生の兆候がある旨を出力する出力手段として機能させることを、特徴としている。

【0021】

また、上記の課題を解決するために、本発明の第2の態様によるルーティンググループ検出プログラムは、以下のような構成を採用した。

【0022】

すなわち、本発明の第2の態様によるルーティンググループ検出プログラムは、コンピュータを、ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出手段、前記パケット抽出手段が抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先IPアドレスを読み取る読取手段、前記読取手段が読み取った送信先IPアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信手段、前記パケット送信手段が送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信手段、及び、前記パケット受信手段が受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティンググループが発生している旨を出力する出力手段として機能させることを、特徴として

いる。

【0023】

これらのように構成されるので、少なくとも2台のルータを備えたとともにルータ同士を隣接させる全ての経路にそれぞれパケットキャプチャ装置が組み込まれたネットワークにおいて、第1の態様によるルーティンググループ検出プログラムが実行された第1のコンピュータに対し、各パケットキャプチャ装置がキャプチャするパケットを監視させ、第2の態様によるルーティンググループ検出プログラムが実行された第2のコンピュータに対し、ネットワーク中の最上流側にあるゲートウェイルータの直後に配置されているパケットキャプチャ装置がキャプチャするパケットを監視させれば、以下のような効果がある。

【0024】

すなわち、ルータ同士を隣接させる全ての経路にそれぞれパケットキャプチャ装置を組み込むことにより、どのルータ間においてルーティンググループが発生しても、その兆候を確実に捕らえることができる。また、或る送信元IPアドレスからのパケットだけがルーティンググループを引き起こしてその他のパケットは引き起こさないという現象が生じた場合でも、そのルーティンググループの発生兆候を確実に捕らえることができる。

【0025】

このとき、第1のコンピュータに対しては、キャプチャされたパケットから残存ホップ数のみを取得させてホップ数毎の度数値をカウントさせるようにしているので、ルータ間の通信速度が高い大規模なネットワークであっても、第1のコンピュータの処理が追いつかなくなるようなことがなくなる。このため、ネットワークの規模の大小に拘わらず、そのネットワーク内の何れかのルータ間で生ずるルーティンググループの発生兆候を、確実に且つ即時に検出することができる。

【0026】

なお、第1のコンピュータによって検出されるルーティンググループの発生兆候には、トレースルートやアタックのような意図的な操作にて生じたものと、意図的な操作ではない純粋な通信障害として生じたものとが、含まれており、第1のコンピュータによっては、両者を区別することはできない。しかし、第1のコンピュータがルーティンググループの発生兆候を検出したときには、その兆候を検出したパケットキャプチャ装置に対応するルータのIPアドレスを第2のコンピュータに通知させれば、その第2のコンピュータが、その通知をトリガーとして、発生源となるルータを含む経路でのルーティンググループの発生を調査することができる。

【0027】

その調査を開始した第2のコンピュータは、ゲートウェイルータを通過するパケットの中から、外部ネットワークへ流出しようとする時間超過メッセージ付きパケットを監視する。そして、その時間超過メッセージ付きパケットを取得した場合には、第2のコンピュータは、その時間超過メッセージ付きパケットを発生させる基となった破棄されたパケットが本来到達すべき送信先IPアドレスを、その時間超過メッセージから読み出し、その送信先IPアドレス宛へ、調査用パケットを送信する。その後、第2のコンピュータは、調査用パケットの応答として、時間超過メッセージ付きパケットが送られてくるか否かを監視し、送られてきた場合には、そのパケットの送信元IPアドレスが、第1のコンピュータから通知されたルータのものであるか否かを確認することができる。

【0028】

このような調査を行う第2のコンピュータに対しては、ゲートウェイルータ直後の経路を通過するパケットの中から、時間超過メッセージを含むパケットだけを取得させるようにしている。この時間超過メッセージ付きパケットは、ルーティンググループによるものの他に、トレースルートやアタックによるものも含まれるが、大きなネットワークにおいては、全パケット中の数割から数パーセントにしか過ぎない。然も、上述した第3の方法のように、パケットの内容が同一であるか否かをいちいち確認しない。このように、第2のコンピュータは、間引かれたパケットについて非常に簡単な処理しか行わずに済むので、ゲートウェイルータ直後のような行き交うパケットの数が非常に膨大な大規模なネット

ワークであっても、時間超過メッセージ付きパケットを確実に捕らえて処理を施すことができる。

【0029】

また、この第2のコンピュータは、時間超過メッセージ付きパケットを取得したときのみ、調査用パケットを送信するので、ネットワークの規模の大小とは無関係に、ネットワークトラフィックに負荷を掛けることがない。然も、このような時間超過メッセージ付きパケットを取得する処理は、第1のコンピュータからの通知を受けたときにしか行わない。従って、ゲートウェイルータ直後の経路には、殆ど負荷が掛かることがない。

【0030】

以上を纏めると、本発明によれば、互いに隣接するルータ同士を繋ぐ全ての経路において、ホップ数毎の度数値からなるヒストグラムが監視され、そのヒストグラムにルーティンググループの発生の兆候が現れた時には、時間超過メッセージ付きパケットの監視と調査用パケットの送信とにより、その兆候の発生源となるルータが検出されるので、確実にルーティンググループを検出することができる。

【0031】

また、本発明によれば、第1のコンピュータに対しては、キャプチャされたパケットからホップ数のみを取得させ、第2のコンピュータに対しては、時間超過メッセージ付きパケットを監視させているだけであるので、規模の大きなネットワークに適用した場合でも、これら第1及び第2のコンピュータが処理を即時に行うことができる。従って、ネットワークの規模の大小とは無関係に、ルーティンググループを即時に検出することができる。

【0032】

なお、本発明においては、調査用パケットは、アプリケーション層上に存在するネットワークアプリケーションサービスについてのサービス要求パケットであっても良いし、エコー要求メッセージを含むパケットであっても良い。

【0033】

前者のようなサービス要求パケットの場合、IPヘッダが付加されるセグメント内のレイヤ4ヘッダにおけるポート番号フィールドの値は、調査用パケットの送り先のノードにおいて開かれているネットワークアプリケーションサービスのポート番号に一致させておくことと良い。こうしておくこと、そのノードに至るまでの経路の途中においてパケットフィルタリングが行われていても、そのパケットフィルタリングによって調査用パケットが経路の途中で破棄されることがない。

【0034】

また、本発明においては、調査用パケットの送り先は、時間超過メッセージから読み取られた破棄対象パケットの送信先IPアドレスであるが、この調査用パケットのプロトコル番号は、この破棄対象パケットのプロトコル番号と一致していると良い。このように、プロトコル番号を一致させる方法としては、そのプロトコル番号を、時間超過メッセージから送信先IPアドレスとともに読み出しおけば良い。このように、調査用パケットに対してプロトコル番号を動的に付与するようにしておくと、調査用パケットの送り先に至るまでの各ルータにおいて動作中の通信サービスのプロトコル番号を、いちいち確認しなくても済むようになる。

【0035】

また、本発明においては、調査用パケットは、所定のパケット送信プログラムによって動的に作成されるものであっても良いが、事前に記憶装置に記憶されていて必要がある場合に読み出されるものであっても良い。後者のように記憶装置に調査用パケットを記憶しておく場合、その調査用パケットは、調査において不変な情報を所定のフィールドに既に有するものであると良い。こうしておくこと、調査用パケットが必要となった場合には、記憶装置から読み出してその所定のフィールドの内容を調査において必要な情報で更新するだけで済むので、パケット送信プログラムをいちいち立ち上げて処理を行わせるような負荷をコンピュータに与えることがなくなる。従って、時間超過メッセージの監視や調査用パケットの送信に係る処理速度をできるだけ高速化することができる。

【0036】

また、本発明は、時間超過メッセージから読み取られる送信先IPアドレスが同一サブネット中のノードを示すものである場合に、その調査用パケットをそれらノードへ繰り返し送信するものであっても良いが、同一サブネット中の1つのノードへ一旦調査用パケットを送信した後、所定期間が経過するまで、そのサブネット中の各ノードへは調査用パケットを送信しないものであっても良い。こうしておく、ルーティンググループやトレースルートやアタックによって同一内容の時間超過メッセージ付きパケットが短期間に大量発生せられる場合であっても、それらについていちいち調査用パケットを生成することが無くなる。そのため、調査回数を抑えることができ、その結果、ネットワークトラフィックに掛かる負荷を軽減することができる。

【0037】

また、本発明は、時間超過メッセージ付きパケットを取得すると、調査対象となるノードが有する様々な条件とは無関係に、そのノードに調査用パケットを送信するものであっても良いが、調査対象となるノードが有する諸条件に応じて調査用パケットを取り止めるものであっても良い。こうしておく、ルーティンググループからの復旧作業中にあるルータや、破棄パケットのプロトコル番号の示すサービスが実際には作動していないノードに関する条件を事前に設定しておけば、不要な調査用パケットをネットワークに流さなくて済むので、ネットワークトラフィックに掛かる負荷を軽減することができる。

【0038】

また、本発明は、調査用パケットの送信に対する応答として時間超過メッセージ付きパケットを受け取ったコンピュータに対し、さらに、トレースルートの手法によって、ルーティンググループを生じさせているルータ及びそのルータに至るまでの経路を特定させるものであっても良い。こうしておく、ルーティンググループを生じさせているルータを確実に特定することができるようになる。

【0039】

また、上記の課題を解決するために、本発明の第1の態様によるルーティンググループ検出方法は、以下のような構成を採用した。

【0040】

すなわち、本発明の第1の態様によるルーティンググループ検出方法は、コンピュータが、ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をIPヘッダ中に有するパケットの個数を、計数する計数ステップと、前記計数ステップにおいて計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別ステップと、前記判別ステップにおいて前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティンググループの発生の兆候がある旨を出力する出力ステップとを実行することを、特徴としている。

【0041】

また、上記の課題を解決するために、本発明の第2の態様によるルーティンググループ検出方法は、以下のような構成を採用した。

【0042】

すなわち、本発明の第2の態様によるルーティンググループ検出方法は、コンピュータが、ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出ステップと、前記パケット抽出ステップにおいて抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先IPアドレスを読み取る読取ステップと、前記読取ステップにおいて読み取った送信先IPアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信ステップと、前記パケット送信ステップにおいて送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信ステップと、前記パケット受信ステップにおいて受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティンググループが発生している旨

を出力する出力ステップとを実行することを、特徴としている。

【0043】

従って、これら第1及び第2の態様によるルーティンググループ検出方法は、上述した本発明の第1及び第2の態様によるルーティンググループ検出プログラムが実行されたコンピュータにより実現されることになる。

【発明の効果】

【0044】

以上に説明したように、本発明によれば、ネットワークの規模の大小に拘わらずルーティンググループを確実に即時に検出することができる。

【発明を実施するための最良の形態】

【0045】

本発明は、或る管理組織が同一の管理ポリシーに従って運用しているネットワーク（いわゆるAS [Autonomous System]）に対して、適用される。すなわち、本発明は、iDC [internet Data Center]の管理するネットワーク、ISP [Internet Service Provider]の管理するネットワーク、企業及び学術団体のイントラネット、WAN [Wide Area Network]、並びに、LAN [Local Area Network]などに対して、適用される。以下では、本発明を実施するための形態の一例として、いわゆるハウジング（コロケーションとも言う）方式にて顧客に対して通信回線やサーバシステムの設置場所を提供するiDCが管理するネットワークに対して本発明を適用した例を、図面に基づいて説明する。

【0046】

図1は、本発明が適用されたネットワークNを概略的に示す構成図である。図1に示されるように、このネットワークNは、複数のルータ10を備えている。各ルータ10は、所定の通信ケーブルを介して接続されており、全体として、ツリー型のネットワークを形成している。なお、このツリーのトップが上流側である。

【0047】

このネットワークNを構成している各ルータ10のうち、最下流のルータ10には、iDCの顧客の管理下にあるサーバシステム20が、接続されている。各顧客のサーバシステム20は、その顧客が自ら構築したシステムであり、単独のサーバコンピュータから構成され、或いは、複数台のサーバコンピュータ、ルータ、スイッチングハブ等から構成される。

【0048】

また、最上流のルータ10は、いわゆるゲートウェイルータとして機能する。なお、他のルータ10と区別するために、図1では、このゲートウェイルータの符号を10'と表記している。このゲートウェイルータ10'には、インターネットIを構成する各ネットワーク（上述したISP、iDS、イントラネット、WAN、LAN）のゲートウェイルータ、或いは、これらゲートウェイルータの接続ポイントとして機能するIX [Internet eXchange]が、高速通信線を介して接続されている。

【0049】

また、このネットワークN内では、OSI [Open System Interconnection] 参照モデルのネットワーク層（レイヤ3）に相当するプロトコルとして、TCP/IP [Transmission Control Protocol/Internet Protocol] スイートに含まれるIP及びICMP [Internet Control Message Protocol] が、用られている。すなわち、このIP及びICMPに従った通信を行うためのプログラムが、各ルータ10のROM [Read Only Memory]等に搭載されている。

【0050】

さらに、このネットワークNは、本発明に係る第1のルーティンググループ検出装置30を、複数備えている。これら第1のルーティンググループ検出装置30は、図1に示されるように、互いに隣接するルータ10同士の間割り込まれることによって、それぞれ、一対のルータ10、10を連絡している。図2は、この第1のルーティンググループ検出装置30を概略的に示す構成図である。

【0051】

第1のルーティンググループ検出装置30は、CPU [Central Processing Unit] 30a, RAM [Random Access Memory] 30b, 通信制御装置30c, 及び、HDD [Hard Disk Drive] 30dを、備えている。

【0052】

CPU 30aは、この第1のルーティンググループ検出装置30全体を制御するための中央処理装置である。RAM 30bは、CPU 30aが各種プログラムを実行するに際しての作業領域が展開される主記憶装置である。

【0053】

通信制御装置30cは、OSI参照モデルのデータリンク層及び物理層に相当するプロトコルに従った通信を司る装置であり、上述したルータ10における当該プロトコルに従った通信を司るデバイスと同等のデバイス（例えばスイッチングハブ）である。

【0054】

HDD 30dは、各種のプログラム及び各種のデータが格納される記憶装置である。このHDD 30dには、オペレーティングシステムプログラムの他、本発明に係る第1のルーティンググループ検出プログラム31, パケットキャプチャプログラム32, 及び、パケット送信プログラム33が、格納されている。

【0055】

第1のルーティンググループ検出プログラム31は、2つのモジュールプログラム31a, 31bとこれらモジュールプログラム31a, 31bの実行を制御するためのプログラムとを、含んでいる。この第1のルーティンググループ検出プログラム31に含まれる2つのモジュールプログラム31a, 31bのうち、一方は、図5を用いて後述する集計プログラム31aであり、他方は、図6を用いて後述する解析プログラム31bである。

【0056】

パケットキャプチャプログラム32は、OSI参照モデルのネットワーク層に位置するプログラムであり、CPU 30aに対し、パケットをキャプチャさせるためのプログラムである。すなわち、パケットキャプチャプログラム32は、通信制御装置30cに対してそれに入力されたパケットを全て受け取らせて上位層へ引き渡させるとともに、受信したパケットと同じパケットを元の経路に戻させるためのプログラムである。なお、このパケットキャプチャプログラム32は、ネットワークNにおける上流側から下流側に向かって流れるパケットのみをキャプチャするように、設定されている。

【0057】

パケット送信プログラム33は、CPU 30aに対し、ネットワーク層より上位の層から引き渡されたセグメントをパケットにカプセル化して通信制御装置30cへ引き渡させるためのプログラムである。

【0058】

なお、パケットキャプチャプログラム32を実行するCPU 30a, 及び、通信制御装置30cは、パケットキャプチャ装置に相当する。図2では、第1のルーティンググループ検出プログラム31とパケットキャプチャプログラム32とが、一台のコンピュータに格納されているように、示されているが、別々のコンピュータに格納されていても良い。この場合、パケットキャプチャプログラム32が格納されるコンピュータは、パケットキャプチャ装置として機能するために、通信制御装置30cを備えることとなる。

【0059】

さらに、このネットワークNは、本発明に係る第2のルーティンググループ検出装置40を、備えている。この第2のルーティンググループ検出装置40は、図1に示されるように、ゲートウェイルータ10'とこれに隣接する2個のルータ10, 10との間に割り込まれることによって、これらルータ10', 10, 10を連絡している。図3は、この第2のルーティンググループ検出装置40を概略的に示す構成図である。

【0060】

第2のルーティンググループ検出装置40は、CPU 40a, RAM 40b, 通信制御装

置 40c, 及び、HDD 40d を、備えている。これらハードウェア 40a~40d は、第 1 のルーティンググループ検出装置 30 のそれらと同等のハードウェアである。

【0061】

但し、HDD 40d には、第 1 のルーティンググループ検出装置 30 の HDD 30d に格納されているプログラムとは一部異なるプログラムが、格納されている。具体的には、HDD 40d には、オペレーティングシステムプログラム、第 2 のルーティンググループ検出プログラム 41、パケットキャプチャプログラム 42、及び、パケット受信プログラム 43 が、格納されている。

【0062】

第 2 のルーティンググループ検出プログラム 41 は、2 つのモジュールプログラム 41a, 41b とこれらモジュールプログラム 41a, 41b の実行を制御するためのプログラムとを、含んでいる。この第 2 のルーティンググループ検出プログラム 41 に含まれる 2 つのモジュールプログラム 41a, 41b のうち、一方は、図 11 を用いて後述する監視プログラム 41a であり、他方は、図 12 乃至図 14 を用いて後述する調査プログラム 41b である。

【0063】

パケットキャプチャプログラム 42 は、第 1 のルーティンググループ検出装置 30 のそれと同様の機能を発揮するものである。但し、第 2 のルーティンググループ検出装置 40 のパケットキャプチャプログラム 42 は、第 1 のルーティンググループ検出装置 30 のそれとは逆に、ネットワーク N における下流側から上流側に向かって流れるパケットのみをキャプチャするように、設定されている。なお、パケットキャプチャプログラム 42 を実行する CPU 40a, 及び、通信制御装置 40c は、パケットキャプチャ装置に相当する。従って、上述したのと同じ理由により、第 2 のルーティンググループ検出プログラム 41 とパケットキャプチャプログラム 42 とは、同一のコンピュータに格納されていても良いし、別々のコンピュータに格納されていても良い。

【0064】

パケット受信プログラム 43 は、CPU 40a に対し、通信制御装置 40c から引き渡されたパケットから IP ヘッダを取り除かせることによってセグメントを生成して上位層へ引き渡させるプログラムである。

【0065】

次に、以上のように構成されるネットワーク N において実行される処理について説明する。なお、以下では、先に、第 1 のルーティンググループ検出装置 30 において実行される処理の内容を説明して、その処理によってなされる作用効果を説明し、その後、第 2 のルーティンググループ検出装置 40 において実行される処理の内容を説明して、その処理によってなされる作用効果について説明する。

【0066】

まず、第 1 のルーティンググループ検出装置 30 において実行される処理の内容について説明する。第 1 のルーティンググループ検出装置 30 では、主電源が投入されると、CPU 30a によって HDD 30d から第 1 のルーティンググループ検出プログラム 31 が読み出され、第 1 のルーティンググループ検出処理が実行される。図 4 は、この第 1 のルーティンググループ検出処理の内容を説明するためのフローチャートである。

【0067】

第 1 のルーティンググループ検出処理の開始後、最初のステップ S101 では、CPU 30a は、時間計測を開始し、ステップ S102 へ処理を進める。

【0068】

ステップ S102 では、CPU 30a は、集計プログラム 31a 及び解析プログラム 31b を実行する。つまり、第 1 のルーティンググループ検出装置 30 には、集計処理プロセス及び解析処理プロセスが、生成される。なお、集計処理プロセス及び解析処理プロセスは、並行に実行される。また、これら集計処理及び解析処理の内容については、図 5 及び図 6 を用いて後述する。これら二つのプロセスの生成後、CPU 30a は、ステップ S1

03へ処理を進める。

【0069】

ステップS103では、CPU30aは、解析処理プロセスが消滅するまで待機する（S103；NO）。そして、解析処理プロセスが消滅すると（S103；YES）、CPU30aは、ステップS104へ処理を進める。

【0070】

ステップS104では、CPU30aは、兆候検出フラグが1であるか否かを判別する。なお、この兆候検出フラグは、解析処理プロセスの実行の結果、0及び1の何れかに切り替えられる。そして、CPU30aは、兆候検出フラグが1でなかった場合（S104；NO）には、ステップS106へ進め、兆候検出フラグが1であった場合（S104；YES）には、ステップS105へ処理を進める。

【0071】

ステップS105では、CPU30aは、この第1のルーティンググループ検出装置30が割り込まされている検査対象の経路について、その両端のルータのIPアドレスと、ルーティンググループの発生の兆候が検出された旨とを含む兆候通知を、第2のルーティンググループ検出装置40へ送信する。なお、この送信では、パケット送信プログラム33による機能が用いられる。送信後、CPU30aは、ステップS106へ処理を進める。

【0072】

ステップS106では、CPU30aは、ステップS101における時間計測の開始時点から所定時間（例えば10分）が経過するまで待機する（S106；NO）。そして、時間計測の開始時点から所定時間が経過すると（S106；YES）、CPU30aは、ステップS101へ処理を戻し、新たに、集計処理プロセスと解析処理プロセスを生成する。

【0073】

従って、第1のルーティンググループ検出装置30では、主電源が投入されている間、ステップS102～S105が、定期的に実行される。

【0074】

図5は、集計処理の内容を説明するためのフローチャートである。この集計処理の開始後、最初のステップS111では、CPU30a（以下、CPU30aが集計プログラム31aを実行することによって実現される機能を、集計処理プロセス31aと表記する）は、時間計測を開始し、ステップS112へ処理を進める。

【0075】

ステップS112では、集計処理プロセス31aは、パケットキャプチャプログラム32（を実行したCPU30aによる機能）から1個のパケットのデータを受け取ったか否かを、判別する。そして、集計処理プロセス31aは、パケットキャプチャプログラム32から1個のパケットのデータを受け取っていなかった場合（S112；NO）には、ステップS115へ処理を進め、パケットキャプチャプログラム32から1個のパケットのデータを受け取っていた場合（S112；YES）には、ステップS113へ処理を進める。

【0076】

ステップS113では、集計処理プロセス31aは、このパケットのIPヘッダ中の生存時間フィールド（IPバージョン6の場合にはホップリミットフィールド）から残存ホップ数を読み取り、ステップS114へ処理を進める。

【0077】

ステップS114では、集計処理プロセス31aは、読み取った残存ホップ数の値を解析処理プロセスへ通知し、ステップS115へ処理を進める。

【0078】

ステップS115では、集計処理プロセス31aは、時間計測を開始してから所定時間（例えば10秒）が経過したか否かを、判別する。そして、所定時間が経過していなかった場合（S115；NO）には、集計処理プロセス31aは、ステップS112へ処理を

戻す。

【0079】

このステップS112～S115の処理ループでは、上流から下流に向かいながら第1ルーティングループ検出装置30を通過する全てのパケットの残存ホップ数が、順次、解析処理プロセス31bへ通知される。そして、この処理ループの実行中、時間計測を開始してから所定時間が経過した場合には、集計処理プロセス31aは、ステップS115からS116へ処理を分岐させる（S115；YES）。

【0080】

ステップS116では、集計処理プロセス31aは、解析処理プロセス31bへ監視終了を通知し、集計処理を終了する。

【0081】

図6は、解析処理の内容を説明するためのフローチャートである。解析処理の開始後、最初のステップS121では、CPU30a（以下、CPU30aが解析プログラム31bを実行することによって実現される機能を、解析処理プロセス31bと表記する）は、RAM30b内のワークテーブルを初期化するとともに、兆候検出フラグを0に切り替えることによって当該フラグを初期化する。

【0082】

なお、ワークテーブルは、IPヘッダの生存時間フィールド（IPバージョン6の場合にはホップリミットフィールド）において取り得るホップ数（255）と同じ数のレコードを、有する。各レコードは、ホップ数のフィールドと、そのホップ数を残存ホップ数として有するパケットの個数を示す度数値のフィールドとを、含んでいる。

【0083】

このステップS121では、解析処理プロセス31bは、このワークテーブル中の全てのレコードの度数値フィールドを0にリセットすることによって、ワークテーブルを初期化する。ワークテーブル及び兆候検出フラグの初期化後、解析処理プロセス31bは、ステップS122へ処理を進める。

【0084】

ステップS122では、解析処理プロセス31bは、集計処理プロセス31aから残存ホップ数の値が通知されているか否かを、判別する。そして、解析処理プロセス31bは、集計処理プロセス31aから残存ホップ数の値が通知されていなかった場合（S122；NO）には、ステップS124へ処理を進め、集計処理プロセスから残存ホップ数の値が通知されていた場合（S122；YES）には、ステップS123へ処理を進める。

【0085】

ステップS123では、解析処理プロセス31bは、ワークテーブルにおける当該ホップ数に対応する度数値を1つカウントアップし、ステップS124へ処理を進める。

【0086】

ステップS124では、解析処理プロセス31bは、集計処理プロセス31aから監視終了が通知されているか否かを、判別する。そして、集計処理プロセス31aから監視終了が通知されていなかった場合（S124；NO）には、解析処理プロセス31bは、ステップS122へ処理を戻す。

【0087】

このステップS122～S124の処理ループでは、集計処理プロセス31aから通知される各パケットの残存ホップ数に基づいて、ワークテーブル内の度数値を順次カウントアップする。そして、この処理ループの実行中、集計処理プロセス31aから監視終了が通知された場合には、解析処理プロセス31bは、ステップS124からS125へ処理を分岐させる（S124；YES）。

【0088】

ステップS125では、解析処理プロセス31bは、ワークテーブル中の各ホップ数とその度数値とに基づいて、度数分布グラフ（ヒストグラム）の曲線における平坦部（又は鋸歯状部）に相当する部分の有無を、検索する。

【0089】

ここで、ワークテーブル中の各ホップ数とその度数値とに基づいて生成され得るヒストグラムについて、簡単に説明する。図7は、ルーティンググループが発生していない場合でのヒストグラムの一例を示し、図8は、ルーティンググループが発生している場合でのヒストグラムの一例を示す。なお、図7及び図8では、度数値の軸は、対数軸となっている。

【0090】

ルーティンググループが発生していない場合、図7に示されるように、ヒストグラムには、幾つかのピークが形成されているとともに、各ピークの脇には、なだらかな曲線状の裾野が形成されている。なお、ピークが出現するのは、パケットに付与する最大ホップ数として各種のOS [Operation System] や装置に設定されているデフォルト値に起因する。デフォルト値としてよく知られているものとして、例えば、windows (マイクロソフト社商標) 系は128、Linux系は64、MacOS (アップルコンピュータ社商標) 系は64と255、ルータは255である。図7においても、ホップ数が128や255である地点の近辺に、ピークが出現している。

【0091】

一方、ルーティンググループが発生している場合、図8に示されるように、ヒストグラムには、図7の場合と同様に、幾つかのピークが形成されているが、各ピークの裾野は、ほぼ平坦になっている。このようにピークの裾野が平坦となるのは、以下の理由に因る。

【0092】

すなわち、隣接するルータ同士で一つのパケットを送受信し続けるという現象がルーティンググループとして最も多く出現するパターンであるが、このパターンでは、第1のルーティンググループ検出装置30は、…、125, 123, 121, 119, …のように、同一のパケットについて2つずつ異なる残存ホップ数をそれぞれ取得することとなる。勿論、3つ以上のルータに跨るようにルーティンググループが発生した場合には、第1のルーティンググループ検出装置30は、等差数列的に値が異なる残存ホップ数をそれぞれ取得することとなる。何れにしても、複数のパケットが同一ルータ間でルーティンググループを発生させた場合には、ヒストグラムにおけるホップ数のグラフ軸における離散的な地点（上記の例で言えば、…、125, 123, 121, 119, …の地点）の度数値が、それらパケットの個数と同じ数になる。このとき、ヒストグラムにおけるピークの裾野は、図9に示されるように、鋸歯状となる。なお、このようにピークの裾野が鋸歯状となるためには、ルーティンググループに突入する前の各パケットが同じ残存ホップ数（或いは、上記の例で言えば奇数の残存ホップ数）を持っていなければならないが、現実には、各パケットの持つ残存ホップ数が揃っていないことが多い。このように残存ホップ数が揃っていなかった場合には、ヒストグラムにおける各ホップ数での度数値は、平均的になる。その結果、ルーティンググループが発生している場合でのピークの裾野は、概ね平坦になる。

【0093】

そして、図6のステップS125では、上述したようなヒストグラムにおける平坦部（又は鋸歯状部）に相当する部分の有無が検索されるが、その検索方法については、様々な手法が知られており、その一例としては、以下のような手法がある。

【0094】

すなわち、その手法を概念的に説明すると、まず、ヒストグラムの度数値の軸を所定数（例えば5）ずつの区間に区分することによって、グラフ曲線を構成する255個のデータを各区間に振り分け、その後、各区間のうち、含まれるデータ数が所定の閾値を超えた区間が存在するか否かを、判別する。そして、所定の閾値を超えた区間が存在した場合に、ヒストグラムに平坦部（又は鋸歯状部）が存在するとして検出する。

【0095】

次のステップS126では、解析処理プロセス31bは、ヒストグラムにおける平坦部（鋸歯状部）に相当する部分が検出できたか否かを、判別する。そして、解析処理プロセス31bは、ヒストグラムにおける平坦部（鋸歯状部）に相当する部分が検出できなかった場合（S126；NO）には、解析処理を終了し、ヒストグラムにおける平坦部（鋸歯

状部)に相当する部分が検出できた場合(S126; YES)には、ステップS127へ処理を進める。

【0096】

ステップS127では、解析処理プロセス31bは、兆候検出フラグを1に切り替えて、解析処理を終了する。

【0097】

以上に説明した第1のルーティンググループ検出処理が実行されることにより、第1のルーティンググループ検出装置30は、以下に説明するように作用する。

【0098】

第1のルーティンググループ検出装置30が割り込まされた経路を上流側から下流側に向かって送信される全てのパケットは、第1のルーティンググループ検出装置30においてキャプチャされる。そして、第1のルーティンググループ検出装置30において解析処理プロセス31bが生成されている期間(S101, S102, S106)において、集計処理プロセス31aが生成されている期間にあるとき(S111, S115)には、キャプチャされた全てのパケットの残存ホップ数が読み取られ(S112~S114)、それに基づいてワークテーブルが生成される(S122, S123)。そして、集計処理プロセス31aによる残存ホップ数の読み取り期間が終了すると(S115; YES, S116, S124; YES)、ワークテーブル中の各ホップ数とその度数値とに基づいて、ヒストグラムの曲線における平坦部(又は鋸歯状部)に相当する部分の有無が検索され(S125)、ヒストグラムの曲線における平坦部(又は鋸歯状部)に相当する部分が検出されると(S126; YES)、この第1のルーティンググループ検出装置30が割り込まされた経路の両端にあるルータのIPアドレスとともに、兆候通知が第2のルーティンググループ検出装置40へ送信される(S105)。

【0099】

つまり、この第1のルーティンググループ検出装置30では、主電源が投入されている間、このような全パケットの残存ホップ数の一定期間での読み取り(S111~S116, S122~S124)と、読み取った残存ホップ数に基づく兆候通知の送信の可否の判定(S125~S127, S103~S105)とが、定期的に繰り返される(S101, S102, S106)。

【0100】

このように作用するために、第1のルーティンググループ検出装置30は、以下に説明するような効果を奏する。

【0101】

すなわち、従来の方法(上述した第3の方法)によれば、監視対象となるパケット全てについて同一内容か否かを一つ一つ検査する必要があった。この検査に必要な1パケット当たりのデータ量は、IPバージョン4においては、13バイト(=識別情報(2バイト)+生存時間(1バイト)+ヘッダチェックサム(2バイト)+送信元IPアドレス(4バイト)+送信先IPアドレス(4バイト))であり、IPバージョン6においては、36バイト(=フローラベル(3バイト)+ホップリミット(1バイト)+送信元IPアドレス(16バイト)+送信先IPアドレス(16バイト))である。しかし、本実施形態の第1のルーティンググループ検出装置30は、全パケットを監視することにはなるとしても、単に各パケットから残存ホップ数(1バイト)を読み取っているだけであり、且つ、ワークテーブル内の度数値をカウントアップさせるという簡易な処理を実行するだけである。然も、全パケットにおける全ての組み合わせについて互いにマッチングするか否かを判別するというような重い処理も行わない。このため、パケットの流入量が非常に膨大であっても、パケットキャプチャ時に、第1のルーティンググループ検出装置30には、処理負荷が殆ど掛からない。つまり、第1のルーティンググループ検出装置30は、隣接するルータ同士を繋ぐ通信回線の通信速度が高速であったとしても、すなわち、大規模なネットワークに適用されたとしても、適切に処理を行える。

【0102】

また、トレースルートによって検出できないルーティンググループ、すなわち、或る送信元から送られたパケットだけがルーティンググループを生じさせてその他のパケットはルーティンググループを生じさせないというようなルーティンググループであっても、そのルーティンググループが第1のルーティンググループ検出装置30を跨いでいれば、その第1のルーティンググループ検出装置30によって確実に検出される。然も、互いに隣接するルータ同士を繋ぐ全ての経路に対し、第1のルーティンググループ検出装置30が割り込まされていることにより、管理区域内で生ずるルーティンググループは、何れかの第1のルーティンググループ検出装置30を必ず跨ぐこととなるので、管理区域内で生ずるルーティンググループは、確実に検出されることとなる。

【0103】

但し、ヒストグラムにおける平坦部（又は鋸歯状部）は、ルーティンググループを生じさせているパケットの他に、トレースルートのために送信されてきた多量のパケットや、互いに異なる残存ホップ数を持ちつつアタックとして送り付けられた多量のパケットによっても、生成される。つまり、ルーティンググループが発生すれば、必ずヒストグラムに平坦部（又は鋸歯状部）が生じるものの、ヒストグラムにおける平坦部（又は鋸歯状部）が、必ずしもルーティンググループを示している訳ではない。従って、第1のルーティンググループ検出装置30は、少なくとも、ルーティンググループの発生兆候を見逃さないと言うことができる。

【0104】

さらに、第1のルーティンググループ検出装置30では、兆候通知の送信の可否の判定を行う時間間隔（S106）を例えば1時間のように長めに設定しておけば、第1のルーティンググループ検出装置30に掛かる処理の負荷やこのネットワークNのトラフィックに掛かる負荷をできるだけ抑えることができ、逆に、その時間間隔を例えば1分のように短めに設定しておけば、ルーティンググループの発生を即時に検出することができる。なお、何れの場合でも、パケットから残存ホップ数を読み取る期間（S115）よりも、兆候通知の送信の可否の判定を行う時間間隔（S106）を短めに設定することが望ましい。

【0105】

次に、第2のルーティンググループ検出装置40において実行される処理の内容について説明する。第2のルーティンググループ検出装置40では、何れかの第1のルーティンググループ検出装置30から兆候通知が、パケット受信プログラム43の機能を通じて受信されると、それをトリガーとして、CPU40aによってHDD40dから第2のルーティンググループ検出プログラム41が読み出され、第2のルーティンググループ検出処理が実行される。図10は、この第2のルーティンググループ検出処理の内容を説明するためのフローチャートである。

【0106】

第2のルーティンググループ検出処理の開始後、最初のステップS201では、CPU40aは、監視プログラム41aを実行する。つまり、第2のルーティンググループ検出装置40には、監視処理プロセスが生成される。

【0107】

図11は、監視処理の内容を説明するためのフローチャートである。監視処理の開始後、最初のステップS211では、CPU40a（以下、CPU40aが監視プログラム41aを実行することによって実現される機能を、監視処理プロセス41aと表記する）は、パケットキャプチャプログラム42（を実行したCPU40aによる機能）から1個のパケットのデータを受け取るまで、待機する（S211；NO）。そして、パケットキャプチャプログラム42から1個のパケットのデータを受け取ると（S211；YES）、監視処理プロセス41aは、ステップS212へ処理を進める。

【0108】

ステップS212では、監視処理プロセス41aは、このパケットが時間超過メッセージ付きパケットであるか否かを、判別する。なお、時間超過メッセージとは、タイプフィールドに11を持つICMPヘッダのことである。このステップS212における処理を

具体的に説明すると、監視処理プロセス41aは、ステップS211においてキャプチャしたパケットがIPヘッダのプロトコル番号フィールドに1を持つか否かを、まず判別し、プロトコル番号フィールドに1を持つ場合には、IPヘッダにはICMPヘッダが付加されているので、そのICMPヘッダのタイプフィールドが11であるか否かを判別する。そして、監視処理プロセス41aは、プロトコル番号が1でない場合、或いは、プロトコル番号が1であるがタイプフィールドが11でない場合、キャプチャしたパケットに時間超過メッセージが含まれていないとして(S212; NO)、ステップS211へ処理を戻し、プロトコル番号が1であってタイプフィールドが11である場合、キャプチャしたパケットに時間超過メッセージが含まれているとして(S212; YES)、ステップS213へ処理を進める。

【0109】

ステップS213では、監視処理プロセス41aは、ステップS211において受信したパケットから、このパケットを発生させる基となったパケットの送信先のIPアドレスを読み取る。具体的には、時間超過メッセージとしてのICMPヘッダのICMPオプションフィールドには、この時間超過メッセージを生成する基となったパケット(すなわち、その宛先に到達する前に残存ホップ数がゼロとなって破棄されてしまったパケット)のIPヘッダとセグメントの一部とが、コピーされており、監視処理プロセス41aは、このICMPオプションフィールドから、本来の送信先IPアドレスを読み取る。読み取り後、監視処理プロセス41aは、ステップS214へ処理を進める。

【0110】

ステップS214では、監視処理プロセス41aは、ステップS211において受信したパケットのICMPオプションフィールドから、その時間超過メッセージを生成する基となったパケットがそのIPヘッダのプロトコル番号フィールドに持っていたプロトコル番号を読み取る。読み取り後、監視処理プロセス41aは、ステップS215へ処理を進める。

【0111】

ステップS215では、監視処理プロセス41aは、ステップS214において読み取ったプロトコル番号が6又は17であるか否かを、判別する。すなわち、監視処理プロセス41aは、当該時間超過メッセージを生成する基となったパケットがTCPヘッダ又はUDP [User Datagram Protocol] ヘッダを持っていたか否かを、判別する。そして、監視処理プロセス41aは、当該プロトコル番号が6又は17でなかった場合(S215; NO)には、ステップS217へ処理を進め、当該プロトコル番号が6又は17であった場合(S215; YES)には、ステップS216へ処理を進める。

【0112】

ステップS216では、監視処理プロセス41aは、ステップS211において受信したパケットのICMPオプションフィールドから、その時間超過メッセージを生成する基となったパケットがレイヤ4ヘッダの送信先ポート番号フィールドに持っていた送信先ポート番号を読み取る。読み取り後、監視処理プロセス41aは、ステップS217へ処理を進める。

【0113】

ステップS217では、監視処理プロセス41aは、調査処理プロセスを実行する。つまり、第2のルーティンググループ検出装置40には、調査処理プロセスが生成される。なお、調査処理プロセスは、この監視処理プロセス41aと並行に実行される。また、調査処理プロセスの内容については、図12乃至図14を用いて後述する。この調査処理プロセスの生成後、監視処理プロセス41aは、ステップS218へ処理を進める。

【0114】

ステップS218では、監視処理プロセス41aは、ステップS213、S214において読み取ったIPアドレス及びプロトコル番号と、ステップS215、S216において読み取れた場合には更にポート番号とを、調査対象情報として、調査処理プロセスへ引き渡す。その後、監視処理プロセス41aは、ステップS219へ処理を進める。

【0115】

ステップS219では、監視処理プロセス41aは、調査処理プロセスが消滅したか否かを、判別する。そして、調査処理プロセスが消滅していなかった場合（S219；NO）には、監視処理プロセス41aは、ステップS220へ処理を進める。

【0116】

ステップS220では、監視処理プロセス41aは、調査処理プロセスから、後述の通知があったか否かを、判別する。そして、後述の通知が調査処理プロセスからなかった場合（S220；NO）には、監視処理プロセス41aは、ステップS219へ処理を戻す。

【0117】

ステップS219、S220の処理ループの実行中、後述の通知が調査処理プロセスからある前に、調査処理プロセスが消滅した場合（S219；YES）には、監視処理プロセス41aは、ステップS211へ処理を戻す。一方、この処理ループの実行中、調査処理プロセスが消滅する前に、後述の通知が調査処理プロセスからあった場合（S220；YES）には、監視処理プロセス41aは、監視処理を終了する。

【0118】

図12及び図13は、調査処理の内容を説明するためのフローチャートである。調査処理の開始後、最初のステップS221では、CPU40a（以下、CPU40aが調査プログラム41bを実行することによって実現される機能を、調査処理プロセス41bと表記する）は、調査対象情報が監視処理プロセス41aから引き渡されるまで、待機する（S221；NO）。そして、調査対象情報を監視処理プロセス41aから受け取ると（S221；YES）、調査処理プロセス41bは、ステップS222へ処理を進める。

【0119】

ステップS222では、調査処理プロセス41bは、監視処理プロセス41aから引き渡された調査対象情報により示される宛先が、調査すべき対象であるか否かを、判別する。

【0120】

なお、調査しなくても良い対象は、HDD40d内に事前に用意されるフィルタリングテーブルにより、管理される。フィルタリングテーブルには、調査しなくて良い対象を選別するための条件としてネットワークNの管理者にて選択されたIPアドレス、プロトコル番号、及び、ポート番号が、登録されている。

【0121】

そして、ステップS222において、調査処理プロセス41bは、調査対象情報中のIPアドレス及びプロトコル番号（存在する場合にはポート番号も）の何れかに一致するものがフィルタリングテーブルに登録されていた場合（S222；NO）には、この調査対象情報により示される宛先が調査すべき対象でないとして、調査処理を終了する。

【0122】

一方、ステップS222において、調査処理プロセス41bは、調査対象情報中のIPアドレス及びプロトコル番号（存在する場合にはポート番号も）の何れもがフィルタリングテーブルに登録されているものと一致しなかった場合（S222；YES）には、この調査対象情報により示される宛先が調査すべき対象であるとして、ステップS223へ処理を進める。

【0123】

ステップS223では、調査処理プロセス41bは、調査対象情報中のIPアドレスが調査を待機すべき対象であるか否かを、判別する。

【0124】

なお、調査を待機すべき対象は、RAM40b内の待機対象管理テーブルにより、管理される。待機対象管理テーブルには、一旦調査対象とされて調査がなされたIPアドレスを含むサブネットのネットワークアドレスであって、その調査から所定待機期間が経過してないものが、登録されている。より具体的には、待機対象管理テーブルには、ネットワ

ークアドレスと待機開始時刻とからなるレコードが、蓄積されている。

【0125】

そして、ステップS223において、調査処理プロセス41bは、調査対象情報中のIPアドレスを含むサブネットのネットワークアドレスが待機対象管理テーブルに登録されていなかった場合(S223; NO)には、当該IPアドレスが調査を即時に開始すべき対象であるとして、ステップS224へ処理を進める。

【0126】

ステップS224では、調査処理プロセス41bは、当該IPアドレスを含むサブネットのネットワークアドレスと、待機開始時刻としての現在時刻とからなるレコードを、RAM40b内の待機対象管理テーブルに登録する。登録後、調査処理プロセス41bは、ステップS227へ処理を進める。

【0127】

一方、ステップS223において、調査処理プロセス41bは、調査対象情報中のIPアドレスを含むサブネットのネットワークアドレスが待機対象管理テーブルに登録されていた場合(S223; YES)には、当該IPアドレスが調査を待機すべき対象であるとして、ステップS225へ処理を進める。

【0128】

ステップS225では、調査処理プロセス41bは、当該IPアドレスを含むサブネットのネットワークアドレスに対応する待機開始時刻から、事前に設定された待機期間(例えば10分)が経過しているか否かを、判別する。そして、調査処理プロセス41bは、当該待機開始時刻から待機期間が経過していなかった場合(S225; NO)には、調査処理を終了し、当該待機開始時刻から待機期間が経過していた場合(S225; YES)には、ステップS226へ処理を進める。

【0129】

ステップS226では、調査処理プロセス41bは、調査対象のIPアドレスを含むサブネットのネットワークアドレスのレコードを待機対象管理テーブルから削除する。削除後、調査処理プロセス41bは、ステップS227へ処理を進める。

【0130】

ステップS227では、調査処理プロセス41bは、調査対象情報に対応する一部作成済パケットを、HDD40dから読み出す。

【0131】

ここで、一部作成済パケットとは、何れの宛先を調査対象とした場合でも不変である情報が各ヘッダの所定のフィールドに予め組み込まれているパケットをいう。この一部作成済パケットは、調査対象に応じて内容を書き換えねばならないフィールドの内容のみを、調査時に書き換えるだけで済ませるためのものである。すなわち、このような一部作成済パケットがHDD40dに事前に格納されていると、図2のパケット送信プログラム33と同等のプログラムに調査用パケットを作成させなくとも、HDD40dから読み出して所定のフィールドの内容を書き換えるだけで、調査用パケットを即時に完成させることができる。

【0132】

なお、本実施形態では、この一部作成済パケットは、プロトコル番号毎に用意されている。つまり、HDD40dには、IPヘッダのプロトコル番号フィールドの内容が互いに異なる一部作成済パケットが、プロトコル番号の数だけ用意されている。但し、一部作成済パケットは、一種類だけ用意されていても良い。何れの場合でも、一部作成済パケットの残存ホップ数は、最大値の255に設定されている。

【0133】

前者のようにプロトコル番号の数だけ用意されている場合、IPバージョン4においては、IPヘッダ中の識別番号フィールド、ヘッダチェックサムフィールド、及び、送信先IPアドレスフィールドが、調査対象に応じて書き換えねばならないフィールドとなり、IPバージョン6においては、IPヘッダ中の送信先IPアドレスフィールドが、調査対

象に応じて書き換えねばならないフィールドとなる。

【0134】

一方、後者のように一部作成済パケットが一種類だけ用意されている場合には、IPバージョン4においては、IPヘッダ中のプロトコル番号フィールドが、更に、調査対象に応じて書き換えねばならないフィールドとして追加され、IPバージョン6においては、IPヘッダ中のネクストヘッダフィールドが、更に、調査対象に応じて書き換えねばならないフィールドとして追加される。

【0135】

また、HDD40dに事前に用意される複数の一部作成済パケットには、何れも、プロトコル番号に応じたレイヤ3ヘッダ（IPヘッダを除く）又はレイヤ4ヘッダが、含まれることとなるが、特に、プロトコル番号が6又は17である一部作成済パケットには、TCPヘッダ又はUDPヘッダのレイヤ4ヘッダが、含まれることとなる。そして、このレイヤ4ヘッダを持つ二つの一部作成済パケットにおいては、さらに、送信先ポート番号フィールド及びチェックサムフィールドが、調査対象に応じて書き換えねばならないフィールドとなる。

【0136】

ステップS227では、調査処理プロセス41bは、調査対象情報中のプロトコル番号（存在する場合にはポート番号も）に対応する一部作成済パケットを、HDD40dから読み出し、ステップS228へ処理を進める。

【0137】

ステップS228では、調査処理プロセス41bは、HDD40dから読み出した一部作成済パケットにおける所定のフィールドの内容を書き換えることにより、調査用パケットを生成する。生成後、調査処理プロセス41bは、ステップS229へ処理を進める。

【0138】

ステップS229では、調査処理プロセス41bは、ステップS228において生成した調査用パケットを、通信制御装置40cへ引き渡すことによって、調査対象情報中のIPアドレス宛へ送信する。送信後、調査処理プロセス41bは、ステップS230へ処理を進める。

【0139】

ステップS230では、調査処理プロセス41bは、調査用パケットの応答としてのパケットを受信するまで、待機する（S230；NO）。なお、この受信には、パケット受信プログラム43による機能が用いられる。そして、調査用パケットの応答としてのパケットを受信すると（S230；YES）、調査処理プロセス41bは、ステップS231へ処理を進める。

【0140】

ステップS231では、調査処理プロセス41bは、調査用パケットの応答として受信したパケットが時間超過メッセージ付きパケットであるか否かを、判別する。そして、調査処理プロセス41bは、受信したパケットが時間超過メッセージ付きパケットでなかった場合（S231；NO）には、調査処理を終了し、受信したパケットが時間超過メッセージ付きパケットであった場合（S231；YES）には、ステップS232へ処理を進める。

【0141】

ステップS232では、調査処理プロセス41bは、調査用パケットの応答として受信したパケットの送信元のIPアドレスが兆候通知中のIPアドレスと同じであるか否かを、判別する。そして、調査処理プロセス41bは、調査用パケットの応答として受信したパケットの送信元のIPアドレスが兆候通知中のIPアドレスと同じでなかった場合（S232；NO）には、調査処理を終了し、調査用パケットの応答として受信したパケットの送信元のIPアドレスが兆候通知中のIPアドレスと同じであった場合（S232；YES）には、ステップS233へ処理を進める。

【0142】

ステップS233では、調査処理プロセス41bは、ループ位置特定処理サブルーチンを実行する。図13及び図14は、ループ位置特定処理サブルーチンの内容を説明するためのフローチャートである。

【0143】

ループ位置特定処理サブルーチンの開始後、最初のステップS251では、調査処理プロセス41bは、RAM40b内のワークテーブルを初期化するとともに、変数Xの値をゼロにする。なお、ワークテーブルは、IPアドレスを格納するためのものである。調査処理プロセス41bは、ワークテーブル内の全てのレコードを削除することによって、ワークテーブルを初期化する。その後、調査処理プロセス41bは、ステップS252へ処理を進める。

【0144】

ステップS252では、調査処理プロセス41bは、変数Xの代入値を1だけインクリメントする。インクリメント後、調査処理プロセス41bは、ステップS253へ処理を進める。

【0145】

ステップS253では、調査処理プロセス41bは、変数Xの代入値が255であるかを、判別する。そして、変数Xの代入値が255でなかった場合（S253；NO）には、調査処理プロセス41bは、ステップS254へ処理を進める。

【0146】

ステップS254では、調査処理プロセス41bは、IPヘッダの生存時間（又はホップリミット）フィールドに変数Xの代入値を持つとともに、エコー要求メッセージを持つパケットを生成する。なお、エコー要求メッセージとは、タイプフィールドに8を持つICMPヘッダのことである。パケット生成後、調査処理プロセス41bは、ステップS255へ処理を進める。

【0147】

ステップS255では、調査処理プロセス41bは、ステップS230において受信したパケットの送信元のノードのIPアドレス宛へ当該パケットを送信し、ステップS256へ処理を進める。

【0148】

ステップS256では、調査処理プロセス41bは、ステップS255において送信したパケットの応答としてのパケットを受信するまで、待機する（S256；NO）。なお、この受信には、パケット受信プログラム43による機能が用いられる。そして、応答としてのパケットを受信すると（S256；YES）、調査処理プロセス41bは、ステップS257へ処理を進める。

【0149】

ステップS257では、調査処理プロセス41bは、受信したパケットがエコー応答メッセージ付きパケットであるかを、判別する。すなわち、タイプフィールドに0を持つICMPヘッダは、エコー応答メッセージと称されているが、調査処理ステップ41は、ステップS257において、受信したパケットにおけるIPヘッダを除く部分にこのエコー応答メッセージが含まれているかを、判別する。そして、受信したパケットがエコー要求メッセージ付きパケットでなかった場合（S257；NO）には、調査処理ステップ41aは、受信したパケットが時間超過メッセージを含むものであるとして、ステップS258へ処理を進める。

【0150】

ステップS258では、調査処理プロセス41bは、時間超過メッセージ付きパケットを送信してきたノードのIPアドレスがRAM40b内のワークテーブルに登録済であるかを、判別する。具体的には、調査処理プロセス41bは、時間超過メッセージ付きパケットのIPヘッダの送信元IPアドレスフィールドからIPアドレスを読み取り、この読み取ったIPアドレスにてワークテーブル内を検索し、そのIPアドレスと同じIPアドレスがワークテーブルから検出できるかを、判別する。そして、時間超過メッセ

ージ付きのパケットを送信してきたノードのIPアドレスがRAM 40b内のワークテーブルに登録されていなかった場合（S258；NO）には、調査処理プロセス41bは、ステップS259へ処理を進める。

【0151】

ステップS259では、調査処理プロセス41bは、時間超過メッセージ付きパケットを送信してきたノードのIPアドレスをワークテーブルに登録する。具体的には、調査処理プロセス41bは、時間超過メッセージ付きパケットのIPヘッダの送信元IPアドレスフィールドからIPアドレスを読み取り、この読み取ったIPアドレスを変数Xの代入値とともにワークテーブルに記録する。記録後、調査処理プロセス41bは、ステップS252へ処理を戻す。

【0152】

ステップS252～S259の処理ループの実行中、変数Xの代入値が255に達してしまった場合には、調査処理プロセス41bは、ステップS253からステップS260へ処理を分岐させる（S253；YES）。

【0153】

ステップS260では、調査処理プロセス41bは、ルーティンググループを発生させているルータの特定に失敗した旨を、監視処理プロセス41aに通知する。通知後、調査処理プロセス41bは、図14のループ位置特定処理サブルーチンを終了するとともに、図12及び図13の調査処理を終了する。

【0154】

また、ステップS252～S259の処理ループの実行中、変数Xの代入値が255に達してしまう前に、エコー要求メッセージ付きパケットの応答としてエコー応答メッセージ付きパケットを受信した場合には、調査処理プロセス41bは、ステップS257からステップS261へ処理を分岐させる（S257；YES）。

【0155】

ステップS261では、調査処理プロセス41bは、ルーティンググループが解消された旨を、監視処理プロセス41aに通知する。通知後、調査処理プロセス41bは、図14のループ位置特定処理サブルーチンを終了するとともに、図12及び図13の調査処理を終了する。

【0156】

また、ステップS252～S259の処理ループの実行中、変数Xの代入値が255に達してしまう前に、IPアドレスがワークテーブルに一旦登録されたノードから再び時間超過メッセージ付きパケットを受信した場合には、調査処理プロセス41bは、ステップS258からステップS262へ処理を分岐させる（S258；YES）。

【0157】

ステップS262では、調査処理プロセス41bは、ワークテーブルにおいて、時間超過メッセージ付きパケットを再び送信してきたノードのIPアドレスを特定し、このIPアドレスからX-1番目のIPアドレスまでの各IPアドレスを、ワークテーブルから読み出す。読み出し後、調査処理プロセス41bは、ステップS263へ処理を進める。

【0158】

ステップS263では、調査処理プロセス41bは、ステップS262において読み出したIPアドレスとともに、ルーティンググループを発生させているルータの特定に成功した旨を、監視処理プロセス41aに通知する。通知後、調査処理プロセス41bは、図14のループ位置特定処理サブルーチンを終了するとともに、図12及び図13の調査処理を終了する。

【0159】

このように、調査処理プロセス41bは、ステップS260、S261、S263の何れかを実行することにより、監視処理プロセス41aへ、ループ位置特定処理の結果である何らかの通知を行うこととなる。なお、上述したように、この監視処理プロセス41aは、調査処理プロセス41bが消滅する前に、調査処理プロセス41bから何らかの通知

を受けると、監視処理を終了する（S220；YES）。但し、調査処理プロセス41bは、ループ位置特定処理サブルーチンを実行せず（つまり何れかの通知をすることなく）に終了することもあり（S222；NO，S225；NO，S231；NO）、この場合（S219；NO）、監視処理プロセス41aは、再び、時間超過メッセージ付きパケットがキャプチャされるのを監視し（S211，S212）、何個目かの調査処理プロセスから通知があるまで監視処理を継続する。

【0160】

一方、図10の第2のルーティンググループ検出処理では、CPU40aは、ステップS201において監視処理プロセスを生成した後、ステップS202において、監視処理プロセス41aが消滅するのを、監視している（S202；NO）。そして、監視処理プロセス41aが何個目かの調査処理プロセス41bからの通知を受けて消滅すると（S202；YES）、CPU40aは、ステップS203へ処理を進める。

【0161】

ステップS203では、CPU40aは、ルーティンググループを発生させているルータの特定に失敗した旨が調査処理ステップ41bから監視処理プロセス41aへ通知されたか否かを、判別する。そして、特定失敗の旨が調査処理ステップ41bから監視処理プロセス41aへ通知されていた場合（S203；YES）には、CPU40aは、ステップS204へ処理を進める。

【0162】

ステップS204では、CPU40aは、ルーティンググループを発生させているルータの特定に失敗した旨とともに、兆候通知に含まれるIPアドレスにより示されるルータにおいてルーティンググループが発生した虞がある旨を、出力する。なお、出力方法としては、例えば、それらの旨を記述した画面をディスプレイ等に表示したり、その旨を記述した電子メールをネットワークNの管理者のパーソナルコンピュータへ送信したりすることができる。出力後、CPU40aは、第2のルーティンググループ検出処理を終了する。

【0163】

一方、ステップS203において、ルーティンググループを発生させているルータの特定に失敗した旨が調査処理ステップ41bから監視処理プロセス41aへ通知されていなかった場合（S203；NO）には、CPU40aは、ステップS205へ処理を進める。

【0164】

ステップS205では、CPU40aは、ルーティンググループが解消された旨が調査処理ステップ41bから監視処理プロセス41aへ通知されたか否かを、判別する。そして、ルーティンググループが解消された旨が調査処理ステップ41bから監視処理プロセス41aへ通知されていた場合（S205；YES）には、CPU40aは、ステップS206へ処理を進める。

【0165】

ステップS206では、CPU40aは、兆候通知に含まれるIPアドレスにより示されるルータにおいてルーティンググループが発生した虞がある旨を、出力する。なお、出力方法としては、上述したのと同様に、ディスプレイ表示や、電子メール送信などすることができる。出力後、CPU40aは、第2のルーティンググループ検出処理を終了する。

【0166】

一方、ステップS205において、ルーティンググループが解消された旨が調査処理ステップ41bから監視処理プロセス41aへ通知されていなかった場合（S203；NO）には、CPU40aは、ルーティンググループを発生させているルータの特定に成功した旨が監視処理プロセス41aに通知されたとして、ステップS207へ処理を進める。

【0167】

ステップS207では、CPU40aは、ルーティンググループが発生している旨と、ルーティンググループの発生箇所が特定できた旨とを、出力するとともに、その発生箇所を示す情報として、監視処理プロセス41aに通知されたIPアドレスを、出力する。なお、出力方法としては、上述したのと同様に、ディスプレイ表示や、電子メール送信などとす

ることができる。出力後、CPU 40aは、第2のルーティンググループ検出処理を終了する。

【0168】

以上に説明した第2のルーティンググループ検出処理が実行されることにより、第2のルーティンググループ検出装置40は、以下に説明するように作用する。

【0169】

第2のルーティンググループ検出装置40は、何れかの第1のルーティンググループ検出装置30からの兆候通知を受けると、監視処理プロセス41を生成することによって、ネットワークNの内部から外部へ流れていく時間超過メッセージ付きパケットを監視する処理を、開始する(S201, S211, S212)。そして、第2のルーティンググループ検出装置40は、時間超過メッセージ付きパケットをキャプチャすると(S212; YES)、ゲートウェイルータ10'から、その時間超過メッセージを生成する基となったパケットの送信先までの経路を、調査対象として特定するため、その送信先に関する情報(送信先IPアドレス、プロトコル番号、送信先ポート番号)を時間超過メッセージから読み取り(S213~S216)、調査処理プロセス41bを生成することによって、調査を開始する(S217, S218, S221)。

【0170】

そして、第2のルーティンググループ検出装置40は、その対象が調査すべき対象であって、且つ、調査を待機すべきでない対象であったときに(S222; YES, S225; YES)、その調査対象に向けて調査用パケットを送信して、応答を待つ(S226~S230)。

【0171】

その応答として時間超過メッセージ付きでないパケットを受信すると、監視処理を再開する(S231; NO, S219; YES, S211, S212)が、その応答として時間超過メッセージ付きパケットを受信すると(S231; YES)、第2のルーティンググループ検出装置40は、そのパケットの送信元が第1のルーティンググループ検出装置30から通知されたIPアドレスと同じであるか判別し(S232)、同じであった場合には、調査対象となる経路においてルーティンググループが発生しているとして、そのルーティンググループを発生させているルータの特定に取り掛かる(S233)。

【0172】

このルータの特定に用いられているループ位置特定処理サブルーチン(S251~S263)には、いわゆるトレースルートの手法が用いられている。すなわち、第2のルーティンググループ検出装置40は、残存ホップ数が互いに異なるエコー要求メッセージ付きパケットを順次調査対象に送信し(S252~S256)、その応答として時間超過メッセージ付きパケットを受信して、そのパケットの送信元ノードのIPアドレスを記録する(S259)。そして、第2のルーティンググループ検出装置40は、エコー応答メッセージ付きパケットが送られてくる前であって、且つ、残存ホップ数が最大値の255に達する前に、同一ノードから時間超過メッセージ付きパケットが繰り返し送られてくるようになってきたときに、記録しておいたIPアドレスの中から、ルーティンググループを発生させているルータのIPアドレスを特定する(S262)。

【0173】

第2のルーティンググループ検出装置40は、このトレースルートの手法により、ルーティンググループを発生させているルータのIPアドレスが特定できたときには(S258; YES)、ルーティンググループを発生させているルータを特定できた旨を出力する(S262, S263, S205; YES, 207)。

【0174】

このように作用するために、第2のルーティンググループ検出装置40は、以下に説明するような効果を奏する。

【0175】

すなわち、従来の方法(上述した第3の方法)によれば、監視対象となるパケット全て

について同一内容か否かを一つ一つ検査する必要があった。この検査に必要な1パケット当たりのデータ量は、上述したように、IPバージョン4においては、13バイトであり、IPバージョン6においては、36バイトである。しかし、本実施形態の第2のルーティンググループ検出装置30は、全パケットを監視することにはなるとしても、IPヘッダのプロトコル番号フィールド(1バイト)が1であるかどうか、プロトコル番号が1である場合にはICMPヘッダのタイプフィールド(1バイト)が11であるかどうかという簡易な処理を行うだけである。然も、全パケットにおける全ての組み合わせについて互いにマッチングするか否かを判別するというような重い処理も行わない。そのうえ、第2のルーティンググループ検出装置40は、ゲートウェイルータ10'から外部に流出しようとするパケットの中から、時間超過メッセージ付きパケットのみを検出し、ゲートウェイルータ10'に流れ込む全てのパケットについて処理を行うわけではない。このため、パケットの流入量が非常に膨大であっても、パケットキャプチャ時に、第2のルーティンググループ検出装置40には、処理負荷が殆ど掛からない。つまり、第2のルーティンググループ検出装置40は、ゲートウェイルータ10'の下流側の通信回線の通信速度が非常に高速であったとしても、すなわち、大規模なネットワークに適用されたとしても、適切に処理を行える。

【0176】

なお、時間超過メッセージ付きパケットは、パケットが消滅したときに生成されるものであるが、このようなパケットの消滅は、ルーティンググループ以外にも、例えば、トレースルートやアタックによっても引き起こされ得る。つまり、ルーティンググループが発生してパケットが消滅したときには、時間超過メッセージ付きパケットが必ず送られてくるものの、時間超過メッセージ付きパケットが必ずルーティンググループの発生を示している訳ではない。従って、第2のルーティンググループ検出装置40は、時間超過メッセージ付きパケットを監視することによって、少なくとも、ルーティンググループの発生の兆候を見逃さないと言うことができる。

【0177】

そこで、この第2のルーティンググループ検出装置40は、時間超過メッセージ付きパケットをキャプチャしたときには、本来の送信先へ調査用パケットを送信する。ここで、再度、時間超過メッセージ付きパケットが返ってきたときには、この時間超過メッセージ付きパケットは、トレースルートやアタック等に因るものではなく、ルーティンググループに因るものであると言える。このため、第2のルーティンググループ検出装置40は、時間超過メッセージ付きパケットのキャプチャ後、本来の送信先へ調査用パケットを送信するだけで、ネットワークN内においてルーティンググループが生じているか否かを、確実に検出することができる。

【0178】

また、第2のルーティンググループ検出装置40は、時間超過メッセージ付きパケットのキャプチャ後、本来の送信先へ即座に調査用パケットを送信する。また、その応答も数秒と掛からずに返ってくる。従って、第2のルーティンググループ検出装置40によれば、ネットワークN内においてルーティンググループが生じたか否かを、即座に確認することができる。

【0179】

また、調査用パケットの応答として時間超過メッセージ付きパケットを受けただけでは、ネットワークN内にルーティンググループが発生していることしか確認できないが、第2のルーティンググループ検出装置40は、調査用パケットの応答としての時間超過メッセージ付きパケットを受信したときには、トレースルートの手法を用いて、ルーティンググループを発生させているルータの特定に掛かる。これにより、ネットワークN内で発生したルーティンググループの発生位置をできるだけ特定することができるようになる。

【0180】

また、第2のルーティンググループ検出装置40では、フィルタリングテーブルに何も定義しておかなければ、時間超過メッセージ付きパケットのキャプチャ後、本来の送信先へ

調査用パケットを必ず送信することとなるが、フィルタリングテーブルに所定の情報を登録しておけば、その条件に合致した送信先へは、調査用パケットが送られることがない。なお、このフィルタリングテーブルに登録する条件としては、例えば、調査の必要が無いノードのIPアドレス、既にルーティンググループが検出されて復旧作業が行われているノードのIPアドレス、本来の送信先において動作していることが有り得ないポート番号などがある。このように、フィルタリングテーブルを用いて、調査用パケットの送り先を制限することにより、ネットワークNに余計な負荷を与えたり、アタックと看做されるようなパケットをネットワークNに送らなくて済む。

【0181】

また、ゲートウェイルータ10'直前を流れる時間超過メッセージ付きパケットは、トレースルートやアタックに因って短期間に大量に発生し、さらには、例えば1つのテキストデータから小分けされた一連のパケットが一つの送信先に送られてそれらが全て同様のルーティンググループに陥ってしまうことによっても短期間に大量に発生する。このように短期間に大量に発生した時間超過メッセージ付きパケットに基づく調査対象は、ほぼ同一のものである可能性が高く、大量に発生する時間超過メッセージ付きパケットの全てについていちいち調査用パケットを送信していたのでは、ネットワークNに負荷を掛けてしまう虞が高い。そこで、第2のルーティンググループ検出装置40では、一旦調査用パケットが送られた送信先のIPアドレスを含むサブネットのネットワークアドレスを、待機対象管理テーブルに登録することにより、一旦調査されたサブネットに対して、一定期間調査用パケットを送られないようにしている。こうすることで、調査回数を大幅に減らすことができ、その結果、ネットワークNへの負荷を軽減することができる。

【0182】

また、第2のルーティンググループ検出装置40では、一部作成済パケットがHDD40dに事前に格納されている。これにより、時間超過メッセージ付きパケットのキャプチャ後、HDD40dから読み出した一部作成済パケットの一部を書き換えれば、即座に調査用パケットを生成することができ、時間超過メッセージ付きパケットをキャプチャする毎にいちいち調査用パケットを新規に生成しなくても済む。その結果、処理速度の低減を防止することができることとなる。

【0183】

また、調査用パケットの送信先やその途中のノードにおいて、セキュリティのために、パケットがIPヘッダ以外に持つデータ（レイヤ4ヘッダ又はレイヤ3ヘッダ）に応じてその通過が制限されていることがある（いわゆるパケットフィルタリング）。この場合、調査用パケットを送信しても、その調査用パケットが途中で破棄されてしまい、適正な応答が返ってこないことがある。これに対し、この第2のルーティンググループ検出装置40は、ゲートウェイルータ10'に流れ込む時間超過メッセージ付きパケットから、その本来の送信先のIPアドレスの他に、プロトコル番号やポート番号を読み取り、そのプロトコル番号やポート番号に対応するデータ（レイヤ4ヘッダ又はレイヤ3ヘッダ）をIPヘッダに付加することにより、送信先において動作している通信サービス（例えば、echo, daytime, telnet, FTP [File Transfer Protocol], ssh [Secure Shell], http [Hyper Text Transfer Protocol], POP [Post Office Protocol], SMTP [Simple Mail Transfer Protocol], DNS [Domain Name Server]）が要求するパケットを生成する。これにより、調査用パケットを送るためのポート等を開けるような作業を本来の送信先に対して行わなくても、パケットフィルタリングによる通過禁止を避ることができ、また、その結果として、その送信先のセキュリティレベルを一時的に低下させることもない。

【0184】

なお、上述した本実施形態では、調査用パケットにおけるIPヘッダに付加されるデータは、本来の送信先についてのプロトコル番号やポート番号に対応するデータ（レイヤ4ヘッダ又はレイヤ3ヘッダ）であったが、これに限られるものではない。この調査用パケットがエコー要求メッセージを含むものである場合を、その変形例として、以下に示す。

【0185】

＜変形例＞

図15は、本実施形態の変形例での監視処理を説明するためのフローチャートである。この図15と図11とを比較して明らかなように、変形例における監視処理は、図11のステップS214～S216を省略したものとなっている。

【0186】

すなわち、監視処理プロセス41aは、パケットキャプチャプログラム42から受け取ったパケットが時間超過メッセージ付きパケットであった場合（S312）、ステップS311において受信した時間超過メッセージ付きパケットのICMPヘッダのICMPオプションフィールドから、このパケットを発生させる基となったパケットの送信先のIPアドレスを読み取り（S313）、その後、直ぐに、調査処理プロセスの生成に取り掛かる（S317）。

【0187】

従って、この変形例においては、監視処理プロセス41aから調査処理プロセス41bへ引き渡される調査対象情報には、本来の送信先のIPアドレスだけが含まれることとなる。

【0188】

一方、変形例における調査処理プロセス41bは、調査対象が待機対象でなかった場合（S225；YES）には、エコー要求メッセージが含まれるように構成された一部作成済パケットをHDD40dから読み出す（S227）。すなわち、変形例における一部作成済パケットは、残存ホップ数として最大値の255を持つIPヘッダと、タイプフィールドに8を持つICMPヘッダとからなっている。調査処理プロセス41bは、このように構成される一部作成済パケットをHDD40dから読み出した後、所定のフィールドを変更し（S228）、調査対象となる宛先へこの調査用パケットを送信し（S229）、その応答を待つ（S230）。

【0189】

このとき、この調査用パケットの応答として送られてくるパケットは、エコー応答メッセージ付きパケットか、時間超過メッセージ付きパケットとなるが、ルーティンググループが発生していることにより送られてくるパケットは、上述した変形前の実施形態と同様に、時間超過メッセージ付きパケットとなる。従って、変形例による第2のルーティンググループ検出装置40も、上述した変形前の実施形態と同様の効果を奏することとなる。読み取り後、監視処理プロセス41は、ステップS214へ処理を進める。

【0190】

（付記1）

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出手段、

前記パケット抽出手段が抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先IPアドレスを読み取る読取手段、

前記読取手段が読み取った送信先IPアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信手段、

前記パケット送信手段が送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信手段、及び、

前記パケット受信手段が受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティンググループが発生している旨を出力する出力手段

として機能させる

ことを特徴とするルーティンググループ検出プログラム。

【0191】

（付記2）

前記調査用パケットは、アプリケーション層上に存在するネットワークアプリケーションサービスについてのサービス要求パケットである

ことを特徴とする付記 1 記載のルーティンググループ検出プログラム。

【0192】

(付記 3)

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数を IP ヘッダ中に有するパケットの個数を、計数する計数手段、

前記計数手段が計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別手段、及び、

前記判別手段が前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティンググループの発生の兆候がある旨を出力する出力手段として機能させる

ことを特徴とするルーティンググループ検出プログラム。

【0193】

(付記 4)

コンピュータが、

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出ステップと、

前記パケット抽出ステップにおいて抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先 IP アドレスを読み取る読取ステップと、

前記読取ステップにおいて読み取った送信先 IP アドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信ステップと、

前記パケット送信ステップにおいて送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信ステップと、

前記パケット受信ステップにおいて受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティンググループが発生している旨を出力する出力ステップとを実行する

ことを特徴とするルーティンググループ検出方法。

【0194】

(付記 5)

コンピュータが、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数を IP ヘッダ中に有するパケットの個数を、計数する計数ステップと、

前記計数ステップにおいて計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別ステップと、

前記判別ステップにおいて前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティンググループの発生の兆候がある旨を出力する出力ステップとを実行する

ことを特徴とするルーティンググループ検出方法。

【0195】

(付記 6)

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出部と、

前記パケット抽出部において抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先 IP アドレスを読み取る読取部と、

前記読取ステップ部において読み取った送信先 IP アドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信部と、

前記パケット送信部において送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信部と、

前記パケット受信部において受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティンググループが発生している旨を出力する出力部とを備えることを特徴とするルーティンググループ検出装置。

【0196】

(付記7)

コンピュータが、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をIPヘッダ中に有するパケットの個数を、計数する計数部と、

前記計数部において計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別部と、

前記判別部において前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティンググループの発生の特徴がある旨を出力する出力部とを備えることを特徴とするルーティンググループ検出装置。

【0197】

(付記8)

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出手段、

前記パケット抽出手段が抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先IPアドレスを読み取る読取手段、

前記読取手段が読み取った送信先IPアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信手段、

前記パケット送信手段が送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信手段、及び、

前記パケット受信手段が受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティンググループが発生している旨を出力する出力手段として機能させる

ルーティンググループ検出プログラムを格納したことを特徴とするコンピュータ可読媒体。

【0198】

(付記9)

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をIPヘッダ中に有するパケットの個数を、計数する計数手段、

前記計数手段が計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別手段、及び、

前記判別手段が前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティンググループの発生の特徴がある旨を出力する出力手段として機能させる

ルーティンググループ検出プログラムを格納したことを特徴とするコンピュータ可読媒体。

【0199】

(付記10)

少なくとも2台のルータを備えるネットワークにおいて、

ルータ同士を隣接させる全ての経路にそれぞれパケットキャプチャ装置を組み込んでおき、

第1のコンピュータが、

前記パケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得

すると、取り得る全てのホップ数のそれぞれについて、そのホップ数をIPヘッダ中に有するパケットの個数を、計数し、

ホップ数毎に計数されたパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別し、

前記ヒストグラムにおいて平坦部又は鋸歯状部があると判別した場合には、そのパケットキャプチャ装置においてルーティンググループの発生が検出されたとして、そのパケットキャプチャ装置に対応するルータのIPアドレスを第2のコンピュータへ通知し、その通知を受けた第2のコンピュータが、

前記ネットワーク中の最上流側にあるゲートウェイルータの直後に配置されているパケットキャプチャ装置において、そのゲートウェイルータから外部ネットワークへ流出するパケットがキャプチャされると、キャプチャされた全てのパケットの中から時間超過メッセージ付きパケットを抽出し、

抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先IPアドレスを読み取り、

読み取った送信先IPアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信し、

送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信し、

受信したパケットが時間超過メッセージ付きパケットであった場合に、そのパケットの送信元のIPアドレスが、前記第2のコンピュータから通知されたルータのIPアドレスと同じであるか否かを判別し、

当該IPアドレスが前記第2のコンピュータから通知されたルータのIPアドレスと同じであると判別した場合に、ルーティンググループがそのルータにおいて発生している旨を、出力する

ことを特徴とするルーティンググループ検出方法。

【図面の簡単な説明】

【0200】

【図1】本発明が適用されたネットワークを概略的に示す構成図

【図2】第1のルーティンググループ検出装置を概略的に示す構成図

【図3】第2のルーティンググループ検出装置を概略的に示す構成図

【図4】第1のルーティンググループ検出処理の内容を説明するためのフローチャート

【図5】集計処理の内容を説明するためのフローチャート

【図6】解析処理の内容を説明するためのフローチャート

【図7】ルーティンググループが発生していない場合でのヒストグラムの一例を示す例示図

【図8】ルーティンググループが発生している場合でのヒストグラムの一例を示す例示図

【図9】ルーティンググループが発生している場合にヒストグラムに出現する鋸歯状部の一例を示す例示図

【図10】第2のルーティンググループ検出処理の内容を説明するためのフローチャート

【図11】監視処理の内容を説明するためのフローチャート

【図12】調査処理の内容を説明するためのフローチャート

【図13】調査処理の内容を説明するためのフローチャート

【図14】ループ位置特定処理サブルーチンの内容を説明するためのフローチャート

【図15】本実施形態の変形例での監視処理を説明するためのフローチャート

【符号の説明】

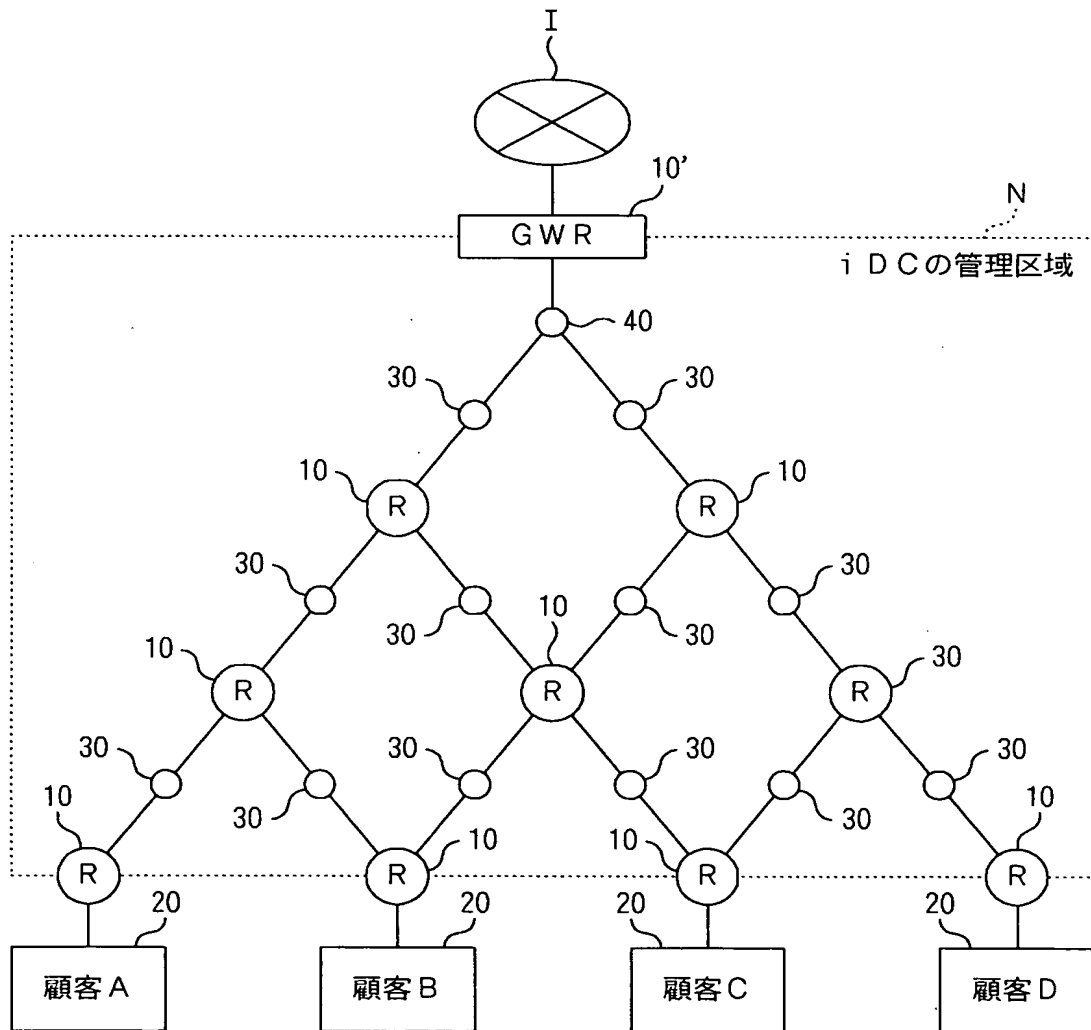
【0201】

10 ルータ

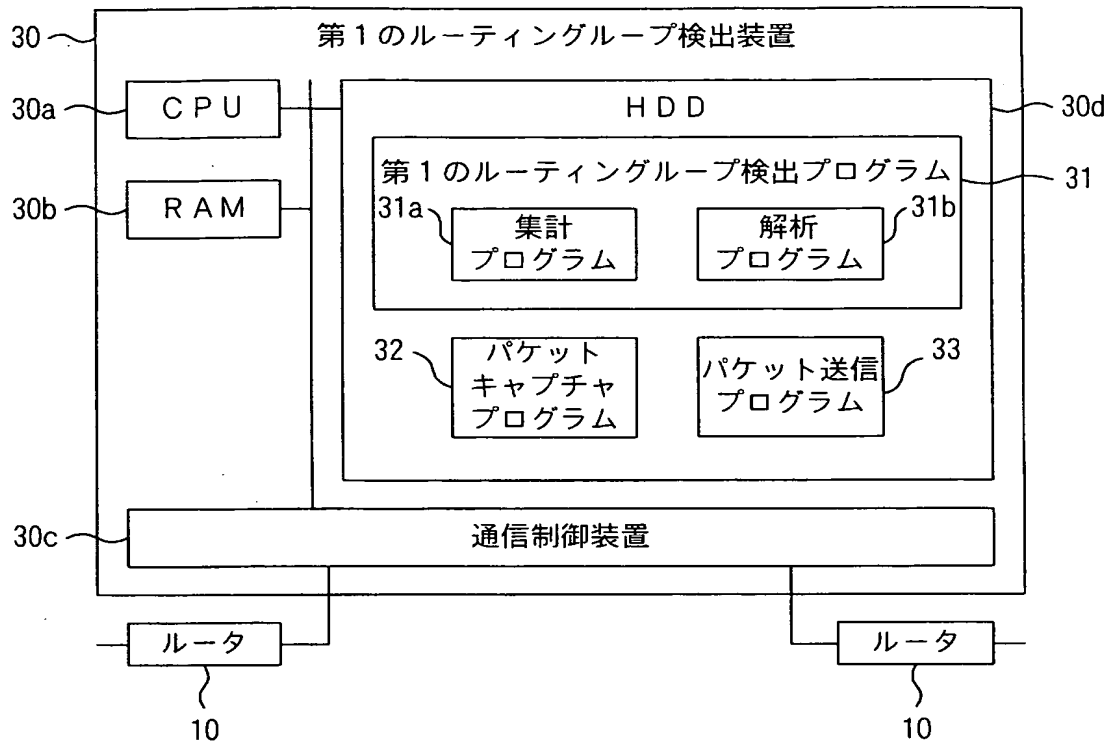
10' ゲートウェイルータ

- 3 0 第 1 のルーティンググループ検出装置
- 3 0 a C P U
- 3 0 b R A M
- 3 0 c 通信制御装置
- 3 0 d H D D
- 3 1 第 1 のルーティンググループ検出プログラム
- 3 2 パケットキャプチャプログラム
- 3 3 パケット送信プログラム
- 4 0 第 2 のルーティンググループ検出装置
- 4 0 a C P U
- 4 0 b R A M
- 4 0 c 通信制御装置
- 4 0 d H D D
- 4 1 第 2 のルーティンググループ検出プログラム
- 4 2 パケットキャプチャプログラム
- 4 3 パケット受信プログラム

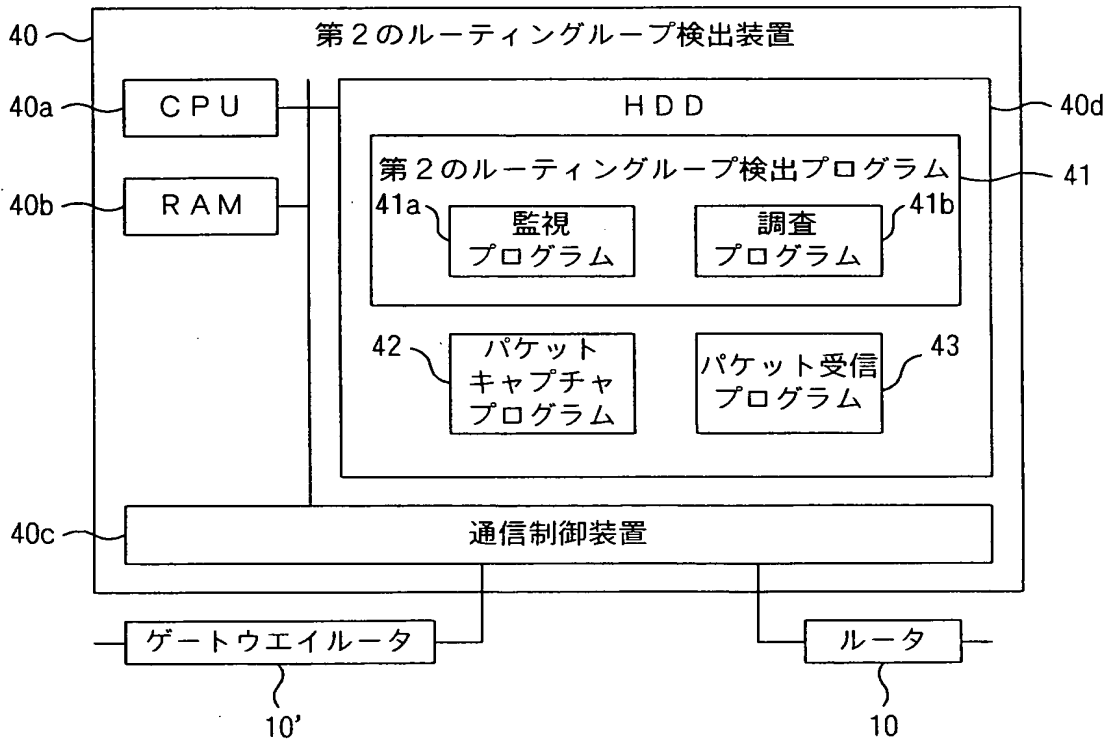
【書類名】 図面
【図 1】



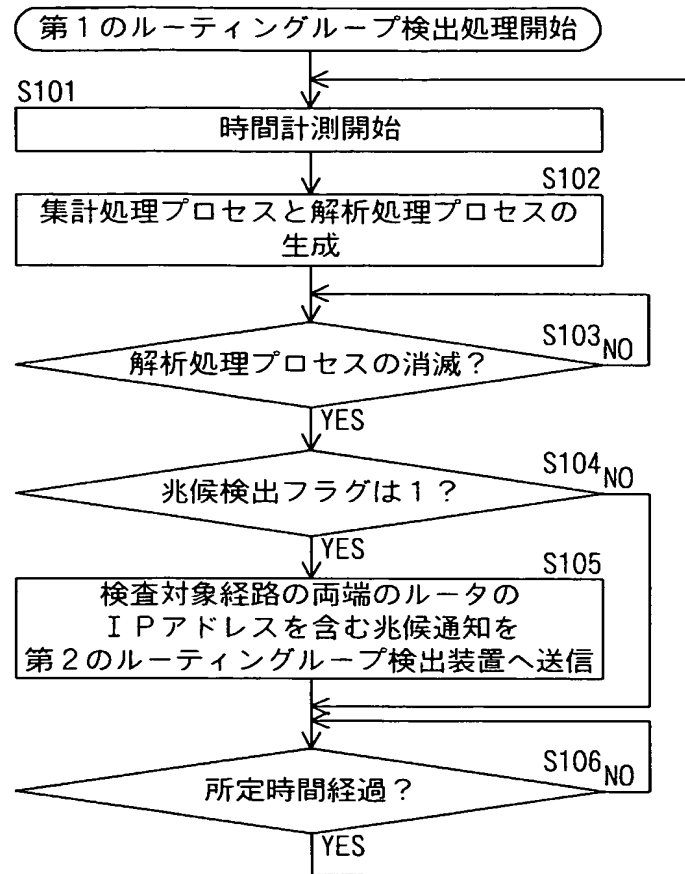
【図 2】



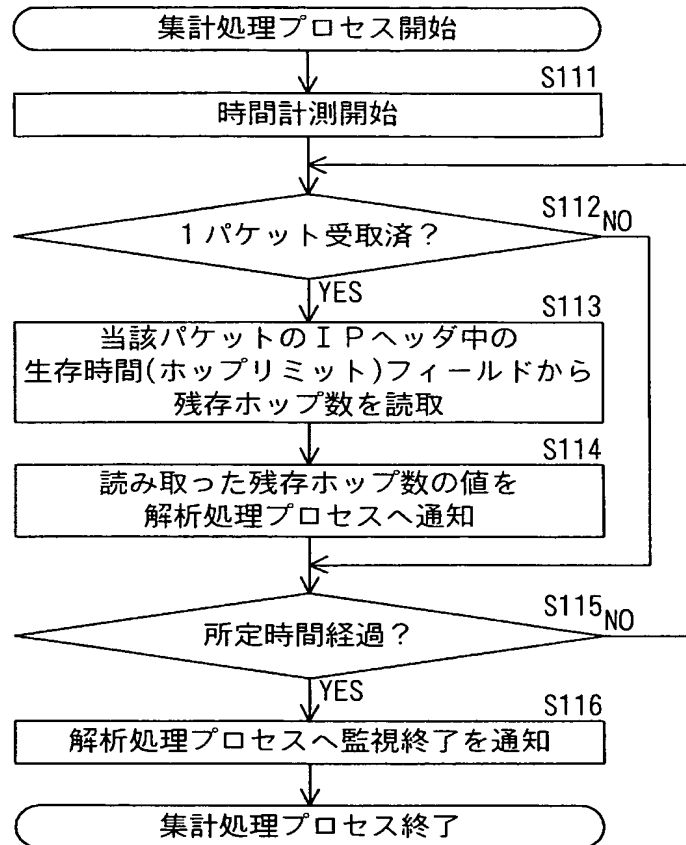
【図 3】



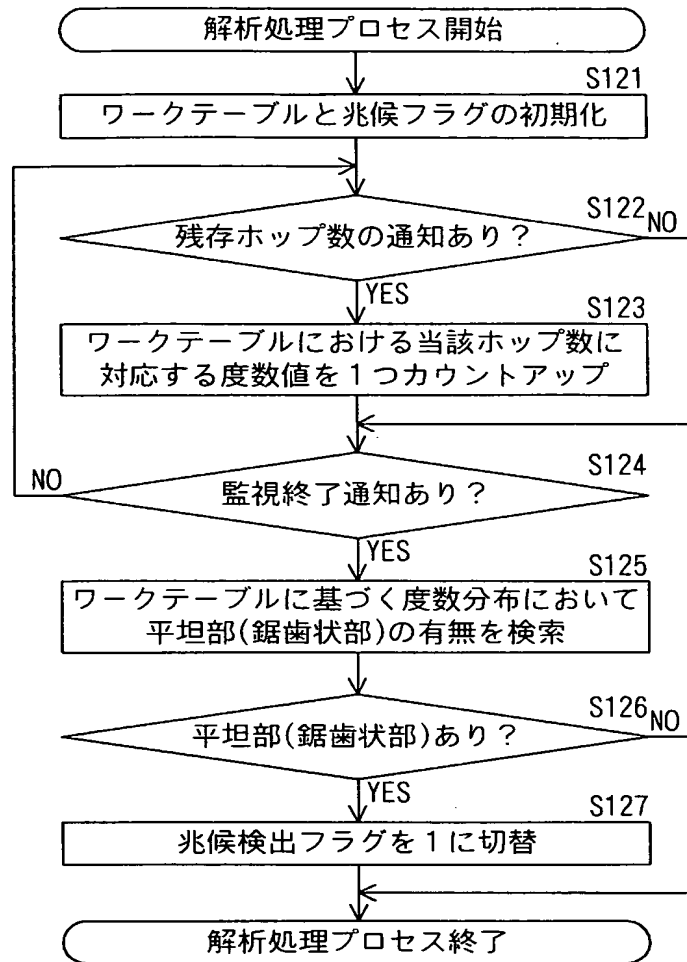
【図 4】



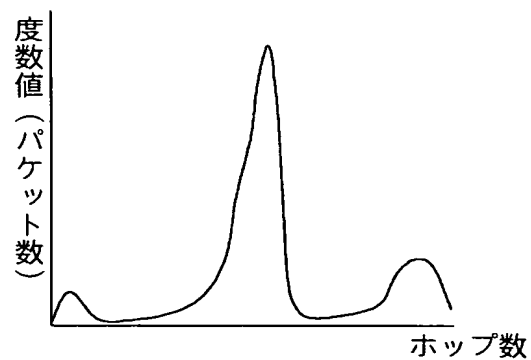
【図 5】



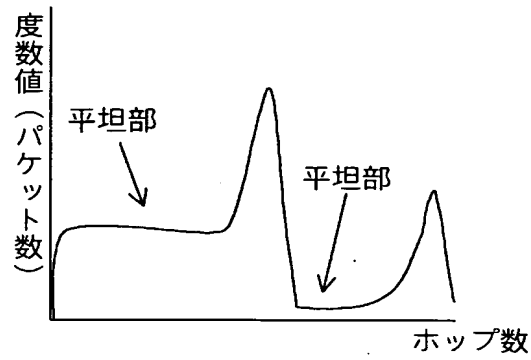
【図 6】



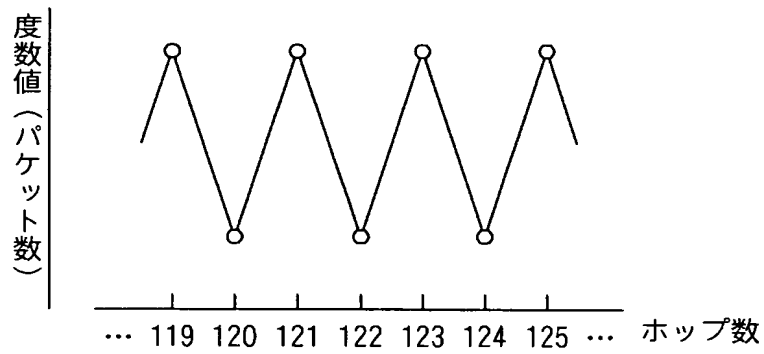
【図 7】



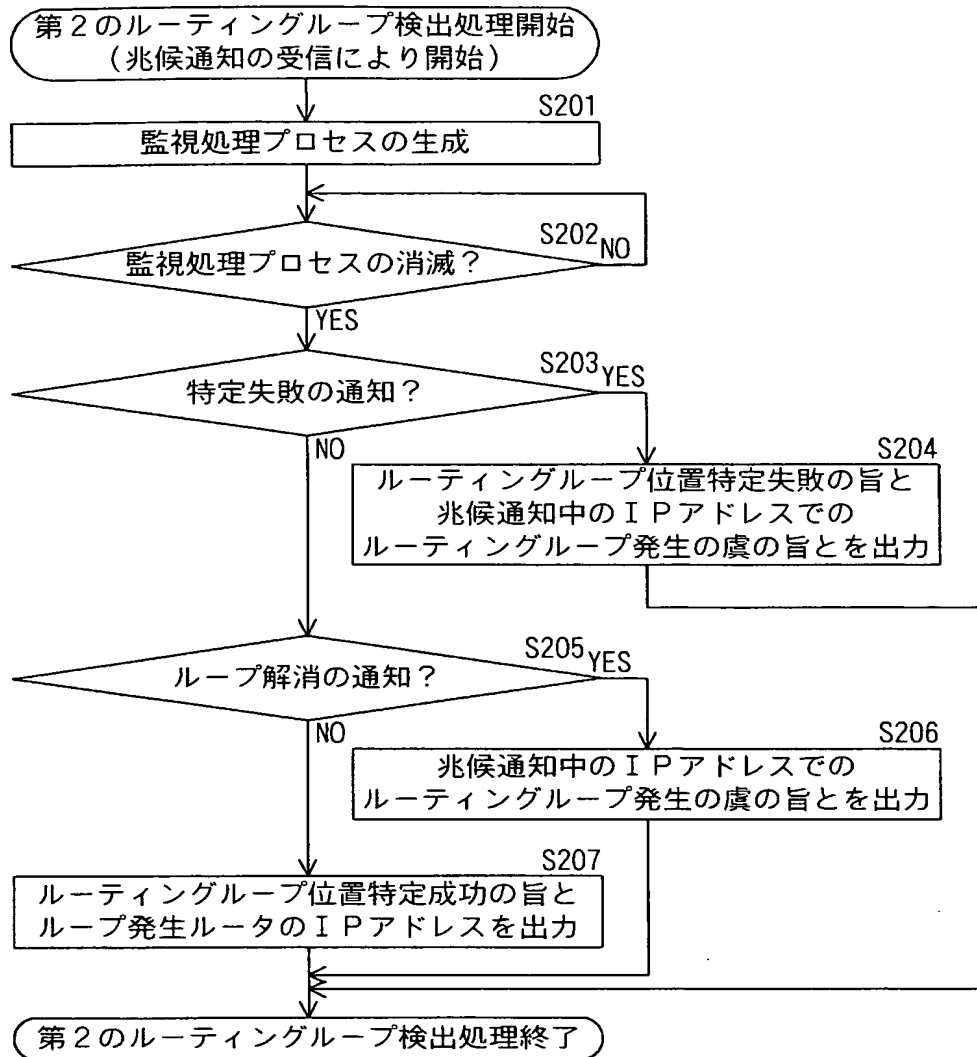
【図 8】



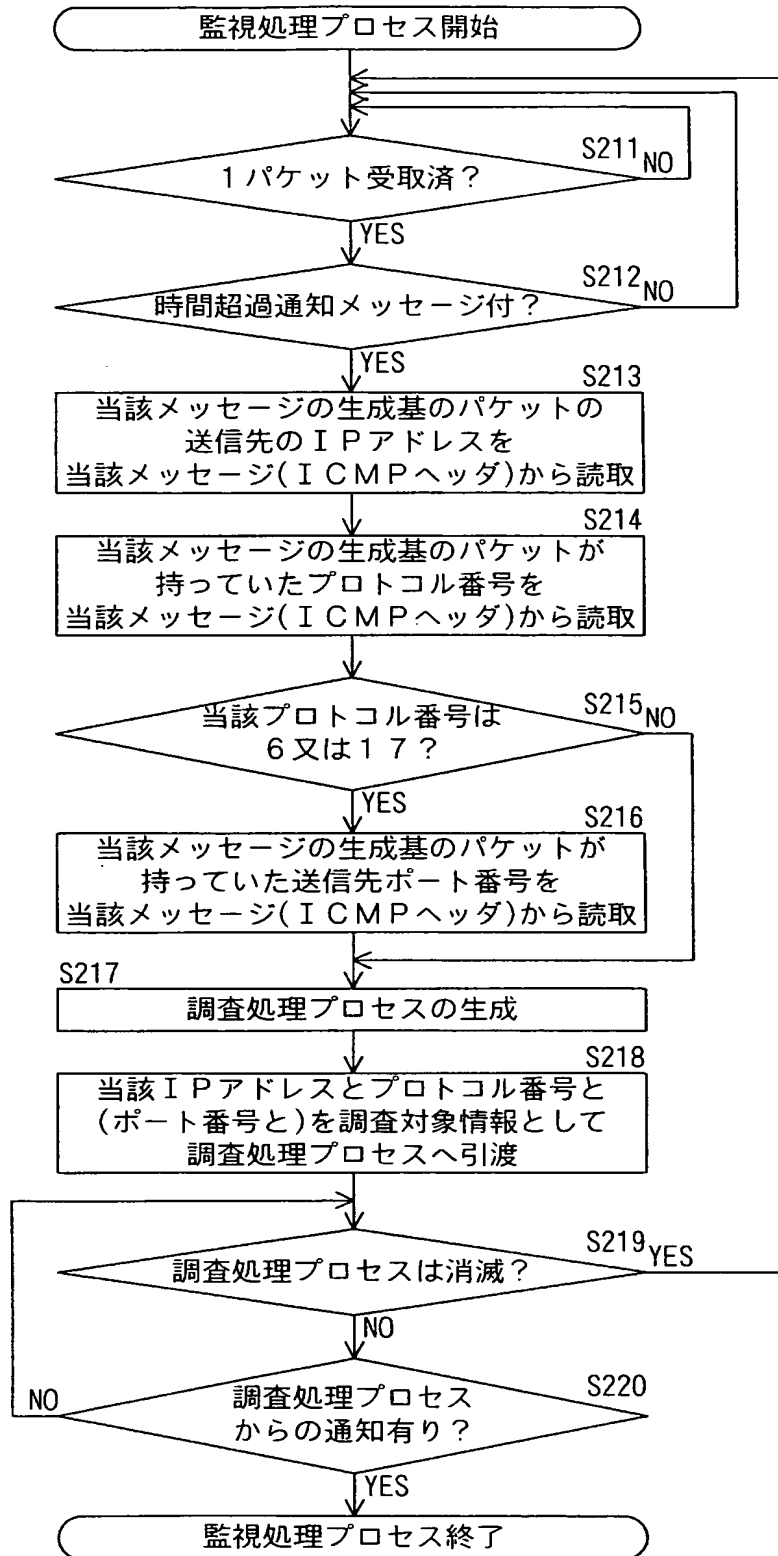
【図 9】



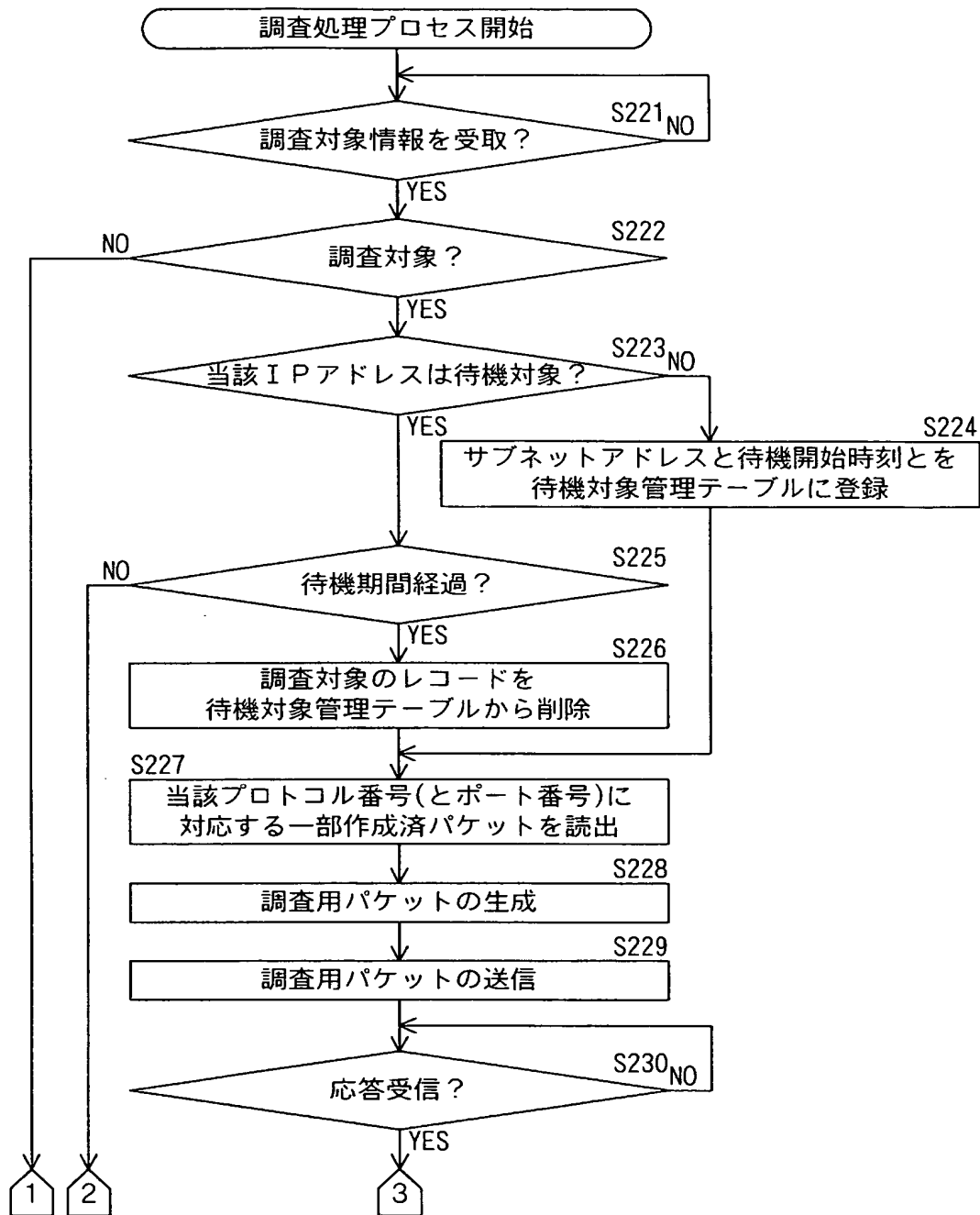
【図 10】



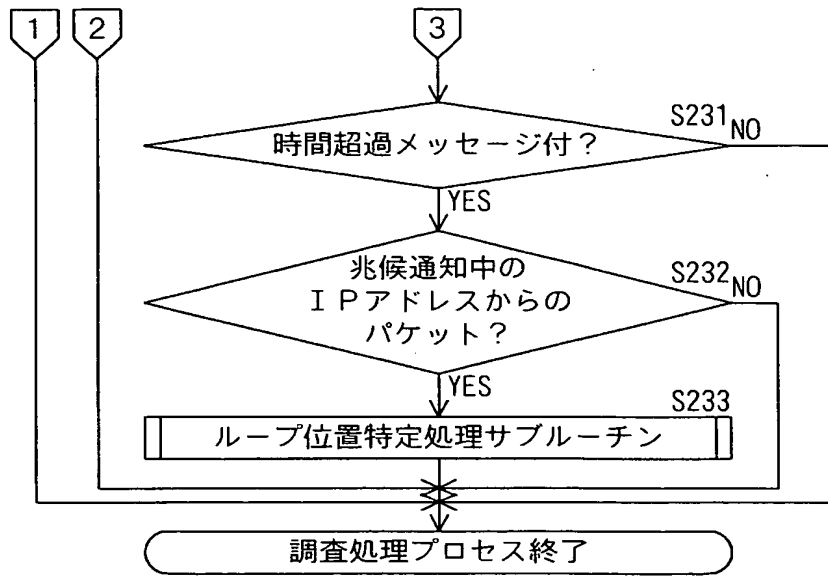
【図 11】



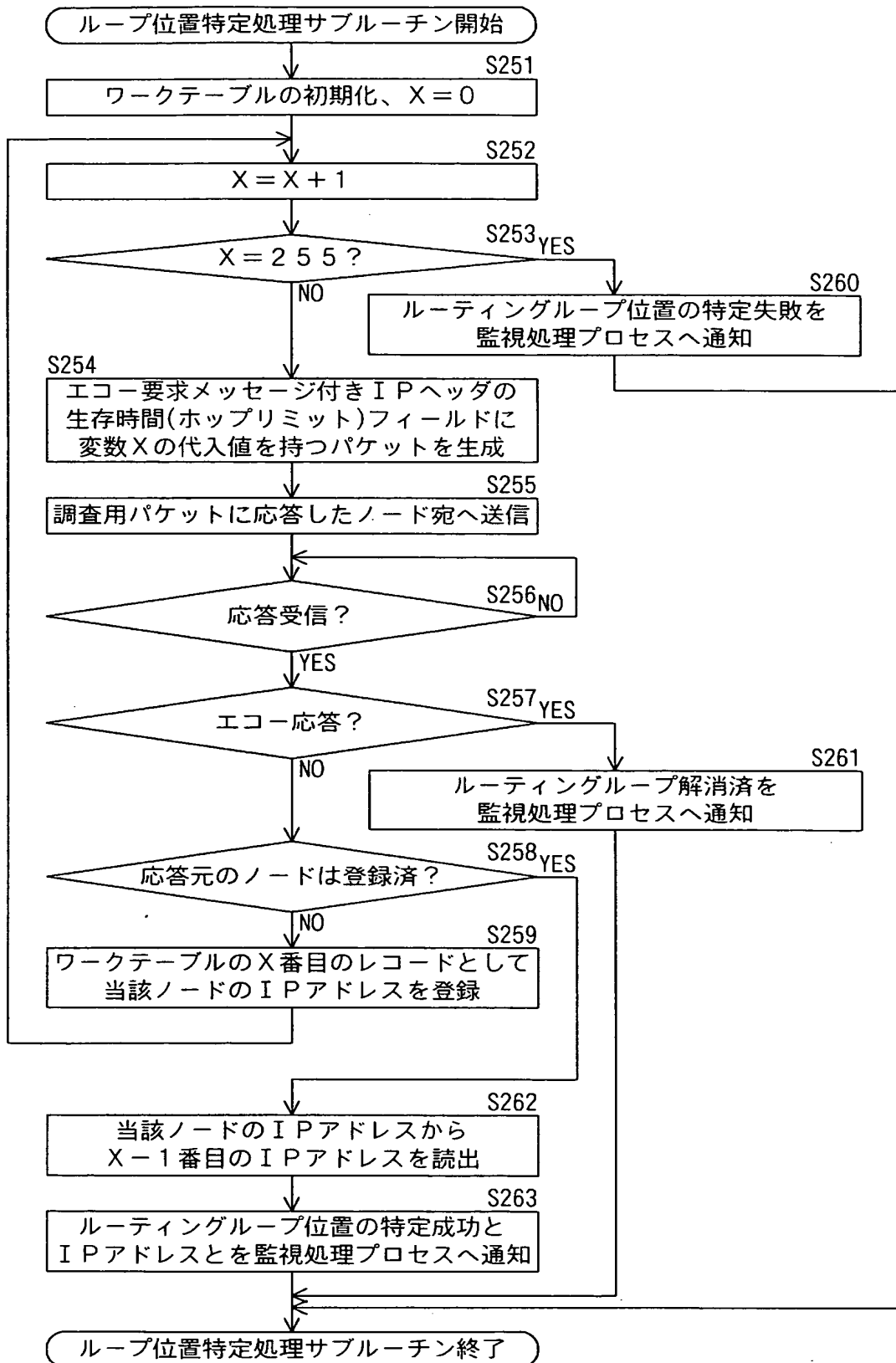
【図 12】



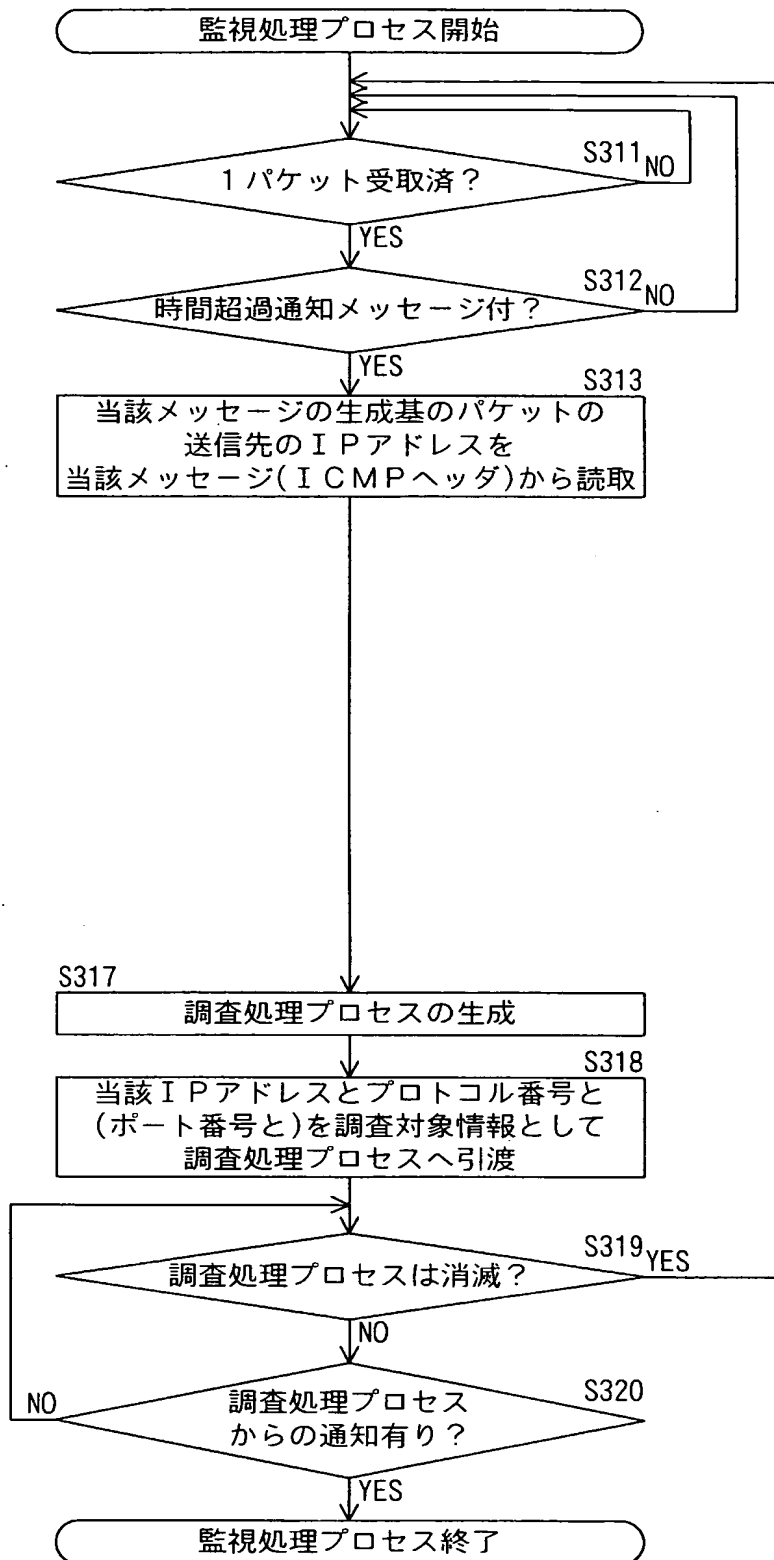
【図 13】



【図 14】



【図 15】



【書類名】 要約書**【要約】**

【課題】 ネットワークの規模に拘わらずルーティンググループを确实且つ即時に検出するためのルーティンググループ検出プログラム及びルーティンググループ検出方法を、提供する。

【解決手段】 第1ルーティンググループ検出装置30は、ネットワークNにおけるルータ10同士を隣接させる全ての経路を下流に向かって流れるパケットを所定期間キャプチャし、ホップ数毎にパケットの個数を計数することによってヒストグラムを生成し、ヒストグラムにおける平坦部分の有無を判別することにより、ルーティンググループの発生を兆候を検出する。第2のルーティンググループ検出装置40は、ゲートウェイルータ10'の下流側においてそのゲートウェイルータ10'から外部へ流出する時間超過メッセージ付きパケットをキャプチャし、元の送信先へ調査用パケットを送信し、その応答として時間超過メッセージ付きパケットを受信することにより、ルーティンググループの発生を検出する。

【選択図】 図1



特願 2 0 0 3 - 3 2 6 1 7 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社